S. HRG. 116–622

THE PACT ACT AND SECTION 230: THE IMPACT OF THE LAW THAT HELPED CREATE THE INTERNET AND AN EXAMINATION OF PROPOSED REFORMS FOR TODAY'S ONLINE WORLD

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, INNOVATION AND THE INTERNET

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JULY 28, 2020

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
52–821 PDF WASHINGTON : 2023

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

ROGER WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
CORY GARDNER, Colorado
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD YOUNG, Indiana
RICK SCOTT, Florida

MARIA CANTWELL, Washington, *Ranking*
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

JOHN KEAST, *Staff Director*
CRYSTAL TULLY, *Deputy Staff Director*
STEVEN WALL, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
RENAE BLACK, *Senior Counsel*

SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, INNOVATION AND THE INTERNET

JOHN THUNE, South Dakota, *Chairman*
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
CORY GARDNER, Colorado
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD YOUNG, Indiana
RICK SCOTT, Florida

BRIAN SCHATZ, Hawaii, *Ranking*
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
EDWARD MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

CONTENTS

WITNESSES

APPENDIX

THE PACT ACT AND SECTION 230: THE IMPACT OF THE LAW THAT HELPED CREATE THE INTERNET AND AN EXAMINATION OF PROPOSED REFORMS FOR TODAY'S ONLINE WORLD

TUESDAY, JULY 28, 2020

U.S. SENATE,
SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY,
INNOVATION AND THE INTERNET,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10 a.m., in room SD–106, Dirksen Senate Office Building, Hon. John Thune, Chairman of the Subcommittee, presiding.

Present: Senators Thune [presiding], Cruz, Fischer, Moran, Gardner, Blackburn, Lee, Schatz, Klobuchar, Blumenthal, Udall, Peters, Baldwin, Tester, and Rosen.

Also present: Senators Wicker, Ex Officio, and Cantwell, Ex Officio.

OPENING STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Good morning. We'll get this hearing underway.

I want to thank everybody for being here today, both virtually and in person. Our panelists today are all appearing virtually, so we look forward very much to hearing from all of you.

We are here to examine the legacy of Section 230 of the Communications Decency Act, which was enacted into law 24 years ago, and to discuss a proposal Senator Schatz and I have introduced to reform Section 230 known as the Platform Accountability and Consumer Transparency Act, or the PACT Act.

Section 230 was written to protect Internet platforms—both large and small—from being held liable for user-generated content while also enabling these platforms to take an active role in moderating such content.

The sweeping nature of these protections, coupled with expansive readings by the courts, has come to mean that, with few exceptions, Internet platforms are not liable for the comments, pictures, and videos that their users and subscribers post, no matter how harmful.

As one of our witnesses here today has written in what he calls his biography of Section 230, the law's proposal and passage flew under the radar back in 1996, receiving virtually no opposition or

media coverage. Today, however, Section 230 is the subject of intense debate and media scrutiny, to the extent that both the President of the United States and his likely competitor in this fall's election have called for the complete repeal of Section 230.

One of many variables that has sparked the intense debate about Section 230 is that Internet platforms have actively cultivated the notion that they are merely providing the technology for people to communicate and share their thoughts and ideas. Therefore, until only relatively recently, the platforms largely concealed, or at the very least failed to disclose, their moderation and curation systems to sustain this fiction of being a neutral platform for all ideas.

Content moderation has, and largely continues to be, a black box, which has led to deep suspicion by many users about bias and discrimination. The reality is that platforms have a strong incentive to exercise control over the content each of us sees, because if they can present us with content that will keep us engaged on the platform, we will stay on the platform longer. Moderation is an important function that platforms must provide in order to deliver a valuable experience to their users. Unfortunately, it's hard for users to get good information about how content is moderated.

The Internet has evolved significantly since Section 230 was enacted. Long gone are the days of the online bulletin boards. Today, Internet platforms have sophisticated content moderation tools, algorithms, and recommended engines to promote content and connect users, all optimized toward keeping every user engaged on the platform.

The platforms have monetized these systems through targeted advertising and related businesses, and have consequently become some of the largest companies in the world. Moreover, these platforms have become essential to our daily lives, as many Americans live, work, and communicate increasingly online. That is why it is important to recognize that the benefits of Section 230 for companies have come with tradeoffs for consumers.

As the Department of Justice has noted in its recommendations to reform Section 230, broad Section 230 immunity can pose challenges for Federal agencies in civil enforcement matters. It is questionable whether Section 230 was intended to allow companies to invoke immunity against the Federal Government acting to protect American consumers in the civil enforcement context. This has contributed to the creation of a different set of rules for enforcing consumer protections against online companies compared to those in the offline world.

In addition, disparate complaint intake and transparency reporting practices between Internet companies have led to a limited ability for consumers to address and correct harms that occur online. And, as Americans conduct more and more of their activities online, the net outcome is an increasingly less protected and more vulnerable consumer.

The Internet of 1996 is a far cry from the Internet of 2020. And, as Americans exist increasingly online, a trend now being accelerated by the COVID–19 pandemic, as illustrated by the fact that each of our witnesses is attending virtually today, reevaluating Section 230 within today's context will ensure its protections continue to balance the interests of both consumers and companies.

Against this backdrop, the bill Senator Schatz and I have introduced would update Section 230 to enable greater transparency and accountability for users without damaging its foundational economic, innovative, and entrepreneurial benefit that helped allow the Internet to flourish in the first place.

The PACT Act would require companies that moderate content to provide a clear and easily accessible user policy that explains how, when, and why user-generated content might be removed. It would also require these online platforms to create a defined complaint system that processes reports and notifies users of moderation decisions within 14 days.

Our legislation would require large technology companies to have a toll-free customer-service phone line with live customer support to take customer complaints. This requirement is geared toward consumers who are less familiar with technology and those in marginalized communities who may not have readily available access to technology, but who want or need to talk to a real person about a complaint about content on a service or platform.

The PACT Act would also hold platforms accountable for their content moderation practices by requiring them to submit quarterly reports to the Federal Trade Commission outlining material they've removed from their sites or chosen to de-emphasize.

In addition, the PACT Act would make it clear that the immunity provided by Section 230 does not apply to civil enforcement actions by the Federal Government. The PACT Act would also make clear that Section 230 does not apply where a platform is provided with a court order finding that content is unlawful.

Both of these provisions are also recommendations that the Department of Justice recently put forward in its recent review of Section 230. At its core, Section 230 reform is about balancing the consumers' need for transparency and accountability against Internet companies' need for flexibility and autonomy. I believe the PACT Act strikes the right balance, and I'm committed to achieving a meaningful bipartisan approach to Section 230 reform that can be enacted into law sooner rather than later.

However, I recognize that the Internet is complex and any meaningful regulation must consider various perspectives from diverse groups in academia, civil society, and industry. Consequently, we have brought together today a very distinguished panel, and I'm confident the conversation will help ensure that we are reforming Section 230 in the right way. Each of our witnesses has deep expertise in both the original intent of Section 230 and how it has been interpreted by the courts over the years.

Today we're joined by former Representative Chris Cox, the coauthor of Section 230 of the Communications Decency Act; Jeff Kosseff, Assistant Professor of Cyber Science at the United States Naval Academy; Elizabeth Banker, Deputy General Counsel of the Internet Association; and Olivier Sylvain, Professor of Law at Fordham School of Law. Thanks to each of you for participating on this important topic.

And I'm now going to recognize Senator Schatz, who will be joining us remotely for his opening statement.

Senator Schatz.

STATEMENT OF HON. BRIAN SCHATZ,
U.S. SENATOR FROM HAWAII

Senator SCHATZ. Thank you, Mr. Chairman, for holding this hearing today to discuss Section 230 of the Platform Accountability and Consumer Transparency Act, the PACT Act.

Before we go any further, I just want to offer some thanks to the Chairman of the Subcommittee, Chairman Thune. Our process has been serious, it has been bipartisan. It is the way the Senate should work. It is the way the Commerce Committee should work. And I'm proud to partner with him on this legislation.

Unfortunately, a lot of the discussion around Section 230 has been focused on provocative but sometimes reactionary and, in some cases, unconstitutional ideas based on the perceived political slights of the day. And there may be some who try to use this hearing as an opportunity to create a clip for social media or to make a few partisan headlines. But, that's not what this hearing is for. We are here to legislate. The work we are doing here today is a serious effort to review Section 230 objectively and on a bipartisan basis, to evaluate how this law should be amended to benefit the American people. This work is already difficult, and it is made much more difficult by grandstanding.

Section 230 was, by all accounts, a prescient and novel idea back in 1996, when it became law. It prevented online platforms from being treated as the publisher or speaker of third-party content, and that avoided liability for their users' content, and, in so doing this, allowed innovators in the United States to create and build products using third-party content without the threat of litigation. This unique idea is one reason why the largest tech companies began in the United States. And, because they started here, many of these platforms became a vehicle for the spread of free speech and democratic ideals across the planet. But, today's Internet is different from when Section 230 is adopted.

And this brings me to a fundamental point. It is OK to update a law. It doesn't mean you think the law was badly written or is deeply, deeply flawed. It just means that, as the Telecommunications Act is periodically amended, as the National Defense Authorization Act is periodically amended, that this law needs to be updated so that it continues to work well.

Now that the Internet has evolved, it is important to ask how Section 230 should evolve along with it. Last month, I introduced the PACT Act with Senator Thune. The bill amends Section 230 and imposes new responsibilities, but not unreasonable ones, on online platforms. It focuses on three concepts: accountability, transparency, and protections for consumers online. To make platforms more accountable to their consumers, the bill requires platforms to respond to consumer complaints about content that is against their own acceptable-use policies or that a court has already determined to be illegal; to improve transparency by requiring platforms to publish reports so that people know what a platform is doing to moderate, based on its own rules; and it increases online consumer protections by fixing the current legal disparities between online and offline commerce and communications.

Some view the debate about Section 230 reform as an opportunity to work the refs or claim bias or make people fearful of the

enforcement of content moderation policies. Our approach has been different. This bill is not targeted at a specific type of content, business model, or company, and its purpose is not to censor or control, or even influence, free speech. Diverse viewpoints make us stronger as a Nation, it's better for the Internet, and I believe that we should preserve robust protections that enable discourse in our country online and offline.

But, I'm proud to be working on such a measured approach to Section 230 reform, and I appreciate the partnership with Senator Thune and his excellent staff. This has been truly a bipartisan effort, and I thank him for the hard work.

Section 230 proponents say that Congress can't possibly change this law without disrupting all of the great innovation that it has enabled. And I just disagree with that. The legislative process is about making sure that our laws are in the public interest, and the PACT Act offers some commonsense changes to the way that the statute functions so consumers have protections, so platforms have accountability and transparency, and so that the statute works today for the Internet.

I want to thank the witnesses for joining us and sharing their expertise on this issue. As part of its jurisdictional oversight on these issues, the Subcommittee looks forward to hearing from you about how the PACT Act's provisions might be a realistic step toward modernizing Section 230. And I look forward to hearing their testimony.

Senator THUNE. Thank you, Senator Schatz. And it has been great partnering with you and your team, and producing something that I think really does represent a good, balanced, sound approach to an issue that has vexed those from all persuasions and perspectives for some time, and I hope that we can make some progress and move this legislation forward.

We are joined today by the distinguished Chairman of the Full Committee, Senator Wicker, and I'm going to recognize him to make some opening remarks.

Senator Wicker.

STATEMENT OF HON. ROGER WICKER,
U.S. SENATOR FROM MISSISSIPPI

The CHAIRMAN. Thank you very much, Mr. Chairman. And I do want to congratulate you and Senator Schatz for working together to solve this matter in a bipartisan fashion.

This is a very important hearing to examine Section 230 of the Communications Decency Act. And I want to extend our thanks and appreciation and welcome to the witnesses for appearing with us remotely.

Section 230 of the Communications Decency Act was enacted in 1996 as part of broader reforms to the Communications Act. Section 230 protects interactive computer services, such as social media platforms, from being held liable for the content posted by their users. Section 230 also specifically allows an interactive computer service, acting in good faith, to restrict the availability of content that it considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable. And I emphasize "otherwise objectionable." The intent of the law, as codified in

the statute, is to preserve a vibrant and competitive online marketplace for the benefit of all Americans. Indeed, a portion of the title chosen by the Subcommittee Chair for this hearing is "The Impact of the Law that Helped Create the Internet." True words.

At the time of its enactment, the Internet was in its infancy. No one could have imagined the success of the digital economy we enjoy today. Section 230 has underpinned much of the Internet's growth and development. It has enabled social media platforms, app developers, websites, bloggers, and others, to host a variety of content and support the free flow of information and ideas without being held legally responsible for the materials generated by users. It has also empowered interactive computer services to remove content that may diminish the safety and security of the Internet.

Despite the vast economic and social benefits of the law, however, I have been deeply troubled by recent reports that suggest some online platforms are disproportionately censoring conservative voices or posing an unfair bias through their policies and terms of service. The administration's executive order on preventing online censorship calls attention to these issues.

As the Committee with jurisdiction over Section 230 of the Communications Decency Act, it is our responsibility to ensure that the law is applied consistently, fairly, and objectively. To ensure greater accountability to the law, this may necessitate a review of these statutes' legal shield for social media companies and others to remove content that they, in their sole discretion, deem to be, quote, "otherwise objectionable." In particular, I question whether this term is too broad and improperly shields online platforms from liability when they remove content that they simply disagree with, dislike, or find distasteful. Such a term may require further defining to reduce ambiguity, increase accountability, and prevent misapplication of the law.

This morning, I hope witnesses will discuss the types of content that fall under the category of "otherwise objectionable." I hope witnesses will also discuss the process by which interactive computer services objectively determine what constitutes "otherwise objectionable content," and how that process is communicated to users in order to preserve a true diversity of political discourse online, as intended by the law. This will help inform the Committee's efforts to maintain a free and open Internet that promotes competition and innovation, and protects multiple viewpoints.

Again, I thank Chairman Thune and Ranking Member Schatz for convening this important hearing.

Thank you.

Senator THUNE. Thank you, Chairman Wicker.

We will now turn to our panel. And, as I mentioned, we have with us a former House member, Chris Cox, a former colleague of both Senator Wicker and I, and delighted to have him back here. We look forward to hearing from you, Chris. He is now speaking here on behalf of NetChoice. As I said, Mr. Jeff Kosseff, Ms. Elizabeth Banker, and Mr. Olivier Sylvain. And my apologies for getting your name wrong the first time.

We'll start with Chris Cox.

Chris, welcome. And it's great to have you here. We look forward to hearing from you. Please proceed.

And I would say, to all of our panelists, to the degree—I know it's hard for you there, probably; you don't have a clock—but, if you could contain or confine your oral remarks to about 5 minutes, it'll maximize the amount of time we have to ask questions and get your responses. And all your comments will be made a part of the permanent hearing record.

So, Mr. Cox, you are recognized.

STATEMENT OF HON. CHRISTOPHER COX, COUNSEL, MORGAN, LEWIS & BOCKIUS, LLP; DIRECTOR, NETCHOICE

Mr. COX. Well, thank you very much, Chairman Thune and Ranking Member Schatz and members of the Subcommittee. Thank you for your invitation to join you in exploring these issues this morning.

I want to apologize for this voice. Since you last heard from me, I've had some surgery that, as an unfortunate side effect, left me with one of my two vocal cords paralyzed. But, I promise to give you, this morning, my full 50 percent.

I should also state at the outset that the views I express this morning are my own and not necessarily those of Morgan, Lewis & Bockius or of NetChoice, where I am a Director.

Those of you who were here in 1995 and 1996 will remember the debate over pornography on the Internet that gave birth to the CDA and, indirectly, Section 230, a quarter century ago. At the time, wayward court decisions really threatened the future of the Internet. A web portal that had done the good deed of screening some user-generated content was being held responsible, therefore, for screening all of it. And, under that unfortunate rule, the good deed of at least trying to keep the Internet free from objectionable material would have been punished.

So, the bill that I wrote to eliminate this perverse incentive, cosponsored by our then House colleague, Ron Wyden, is what eventually became what we now know as Section 230. Looking across the intervening decades of judicial interpretation of Section 230, we can see that the law has contributed directly to the success of the Internet by providing a legal foundation for user-generated content today shared not just among millions, but billions, of people.

We think about the remarkable accomplishment of Wikipedia, something that many of us use almost daily and take for granted, it's long since outstripped the information that was contained in the once unparalleled Encyclopedia Britannica. It's just one marvel of the 21st century that we take for granted. Wikipedia relies entirely upon user-generated content. It's operated by the Wikimedia Foundation, which is, itself, a small organization funded by voluntary contributions. If it were subject to lawsuits for the contributions and comments of its volunteers and users, it couldn't sustain itself, and it would cease to exist as an invaluable free resource for every American.

The fundamental objective of Section 230 has always been to protect the innocent and punish the guilty. The law achieves this objective by protecting websites that host user-created content when, in good faith, they become involved in content creation for the purpose of keeping objectionable material off of their sites, or editing content created by others, or taking it down altogether in order to

remove offensive material. To this extent, the law says they will not be treated as publishers.

At the same time, Section 230, as written and as interpreted today, makes clear that becoming involved in content creation for any other purpose eliminates any protection from suit. And that's true even if the involvement in content creation is only partial. And it's true even if the Internet platform doesn't, itself, create the content, but only develops it. And when the platform is only partly responsible for the mere development, not necessarily the creation, it still loses its Section 230 protection. If a website is in any way complicit in the creation or development of illegal content, it has no Section 230 immunity. The inclusion of this clear language in the statute was absolutely deliberate. It was intended to ensure that both criminal and civil laws would continue to be vigorously enforced. And that's why Section 230 expressly states that Federal criminal law is entirely unaffected by its provisions, and neither is there any effect on the enforcement of State law, whether civil or criminal, provided that the State laws are enforced consistently with the uniform national policy expressed in Section 230.

That uniform national policy applies equally to all civil and criminal offenses. It's important that there be a uniform national policy, because the Internet is the quintessential vehicle of interstate commerce, and its packet-switched architecture makes it uniquely susceptible to multiple sources of conflicting State and local regulation. Even an e-mail from this hearing room to someone in the Capitol across the street can be broken up into pieces and routed through servers in different states. If every state were free to adopt its own policy governing when an Internet platform will be liable, not only would compliance become oppressive, but the Federal policy itself would quickly become undone.

Section 230 changed none of the legal responsibilities of any individual or business or nonprofit. The same legal rules continue to apply on the Internet, just as in the offline world. What Section 230 added to the general body of law was the principle that an individual or entity operating a website could not, in addition to its own legal responsibilities, be required to monitor all of the content created by third parties in order to avoid becoming derivatively liable for the illegal acts of other people.

Congress recognized that to require otherwise would deprive all of us of the essential benefit of the Internet: the opportunity for realtime communication among millions of people around the world. Section 230 succeeded in safeguarding this quintessential aspect of the Internet. Today, there are over 370 million active websites hosted in America, and over 875 million websites accessible to American users.

But, despite the tremendous variety this represents, most of the legislation now being drafted in the House and in the Senate to regulate these websites seems focused on a very different paradigm and a much smaller group of companies. The paradigm of what needs to be regulated seems to be an enormous rapacious company interested only in manipulating its customers or strangling democracy in America. That doesn't come close to describing even the largest e-commerce sites, which are mostly the traditional brick-and-mortar companies, including Kohl's, Target, Costco, and

Walmart, and the Big Tech paradigm certainly doesn't describe the hundreds of thousands of other websites, of all sizes, that bring us user-created content every day. Yet all of these websites, and, more importantly, all of us who are their users, rely on the protection of Section 230 to have access to the many services they provide.

So, as you consider whether—and, if so, how—to legislate in this area, it's important to remember just how much human activity is encompassed within this vast category we so casually refer to as "the Internet." To the extent that any new legislation imposes too much compliance burden or too much liability exposure that's connected to a website's hosting of user-created content, the risk is that too many websites will be forced to respond by getting rid of user-generated content altogether or else scaling it way back. Either way, millions of Internet users in the United States would feel the loss immediately.

I feel confident in saying that if writing Section 230 a quarter century ago was a daunting undertaking, amending it today presents a far greater challenge. Any changes you make will affect every business, every nonprofit, and every individual in America in some ways that you can't even predict and that will inevitably disappoint you.

For that reason, I commend all of you on this committee for taking the thoughtful approach that you are and making every effort to inform yourselves about the endless real-world consequences before legislating in this area.

I look forward to your questions.

[The prepared statement of Mr. Cox follows:]

PREPARED STATEMENT OF CHRIS COX, FORMER U.S. REPRESENTATIVE, AUTHOR AND CO-SPONSOR WITH SENATOR RON WYDEN, SECTION 230

Chairman Thune, Ranking Member Schatz, and Members of the Subcommittee, thank you for the invitation to testify on the history of Section 230 and its application by the courts over the last quarter century. This experiential base is an important starting point as you consider ways to ensure that platforms are accountable for their content moderation practices, and what legislative measures, from transparency to accountability tools, can empower consumers online.

My abiding interest in this subject dates, of course, to some twenty-four years ago when I joined then-Rep. Ron Wyden in writing what today is known as Section 230. In the intervening quarter century I have followed the developments in the case law, sometimes with awe and occasionally with disappointment. The views I express today are my own, and not necessarily those of NetChoice, on whose board I serve, or of Morgan, Lewis & Bockius.

Introduction

As we consider the issues surrounding free expression and content moderation on the internet, it is worth asking: what would our world be like without Section 230?

This is an important question because, to a degree most of us fail to recognize, we take its many benefits for granted. An endless variety of useful and important content on the Internet is supplied not by websites or social media platforms, but by their millions of users who create the content themselves and freely share it. Without Section 230, millions of American websites—facing unlimited legal liability for what their users create—would not be able to host user-generated content at all.

In this way, moreover, Section 230 facilitates every individual's ability to publish their own content on the internet. The wide variety of online forums for posting user-created content is the direct result of the protection from liability for the host sites that Section 230 affords.

At the same time that Section 230 has enabled an endless diversity of voices to reach far greater audiences than was ever possible before, this same law has helped websites to maintain civility and fair play through the application of bespoke standards of content moderation. In contrast to other nations, in the United States the

government does not dictate what can be published on the Internet and who can publish it. The proliferation of websites, each free to adopt their own rules of the road, has simultaneously provided unparalleled opportunities for any individual to reach millions of people around the world—and the means by which offensive online conduct including bullying and obscenity, as well as outright criminal activity, can be restricted without fear of legal liability.

Before the enactment of Section 230, Internet platforms faced a terrible dilemma. If they sought to enforce even minimal rules of the road in order to maintain civility and keep their sites free from obscenity and obnoxious behavior, they became unlimitedly liable for all of the user-created content on their site.[1] On the other hand, if the website followed an "anything goes" business model, with no content moderation whatsoever, then it could completely avoid that liability.[2] From the perspective of any Internet platform that attempted to maintain a family-friendly site, it was a classic case of "no good deed goes unpunished."

Section 230 eliminated the perverse incentive for "anything goes." By imposing liability on criminals and tortfeasors for their own wrongful communications and conduct, rather than shifting that liability to a website that did not in any way participate in the wrongdoing, it freed each website to clean up its corner of the internet. No longer would being a "Good Samaritan" buy trouble.

In an imagined future world without Section 230, where websites and Internet platforms again face enormous potential liability for hosting content created by others, there would again be a powerful incentive to limit that exposure. Online platforms could accomplish this in one of two ways. They could strictly limit user-generated content, or even eliminate it altogether; or they could adopt the "anything goes" model that was the way to escape liability before Section 230 existed.

We would all be very much worse off were this to happen. Without Section 230's clear limitation on liability it is difficult to imagine that most of the online services on which we rely every day would even exist in anything like their current form.

As Congress considers whether to amend Section 230, therefore, it is important to keep in mind the many aspects of the modern Internet we take for granted, and that are dependent upon Section 230's protections. Compromising those protections risks a wide array of unintended consequences. Among these are loss of much of the rich content provided every day by millions of individual content creators, loss of the ability to use social media for real time communication with friends and family, loss of opportunities for diverse voices to reach broad audiences throughout the Nation and across the planet, and damage to e-commerce and the continued technological development of the internet.

In the 21st century, Section 230's protection of website operators from liability for content created by their users operates as an essential buttress of free expression. It is the key to millions of Americans' ability to share news and views and gain instant access to a wide range of informational and educational resources. It is the foundation supporting e-commerce sites such as Yelp, eBay, Facebook, Wikipedia, Amazon, Twitter, and the entire Web 2.0 revolution whereby thousands of innovative platforms offer a range of useful services powered by user-generated content. From user-created reviews of products and services, to educational videos, to online resources that help locate loved ones after natural disasters, to the many online services that have come to the rescue of millions of Americans quarantined or in self-isolation during the Covid pandemic, all of the rich variety now available at our fingertips is precisely what Section 230 was designed to facilitate.

But while Section 230 has been a boon to users of the Internet and to the continued technological and commercial development of the Internet itself, it is not a panacea. We are all familiar with the many pathologies that continue to fester in corners of the dark web, and that too often leach onto the mainstream Internet websites and platforms we rely on every day. Continued challenges to a free and open Internet include the threat of hidden platform "censorship" and undisclosed viewpoint discrimination; "fake news" and content manipulation by bad actors; defamation, cyberstalking, and revenge porn; fraud on consumers; internet-facilitated criminal gang activity; cross-border terrorism; child sexual abuse and sex trafficking; and widespread censorship and social control by dictatorships and authoritarian governments including not only Russia and China, but scores of other nations besides.

Section 230 has not prevented these affronts, but neither is it the cause of them. In many cases, it has helped mitigate their consequences. Preserving the law's benefits for Internet users, society, and the Nation's economy should remain an over-

---

[1] *Stratton Oakmont v. Prodigy Servs. Co.,* 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995).
[2] *Cubby, Inc. v. CompuServe, Inc.,* 776 F. Supp. 135, 140 (S.D.N.Y. 1991).

arching objective of any legislation to address the many looming concerns across the rapidly-evolving landscape of the internet.

In that respect, we will be well advised to recognize the danger of unintended consequences that would accompany efforts to reopen Section 230 to further amendment. There are many competing interests at stake, both commercially and politically, in the constellation of issues affected by Section 230. As each of you is fully aware, the various criticisms of Section 230 come from disparate quarters, and are based on radically different rationales. For example, while some critics demand more robust content moderation, their political opposites demand less interference with user-created content. The process of turning a bill into law in these circumstances will require potentially trenchant compromises.

The multiplicity of stakeholders, including competing business interests, affected by any new legislation governing activity on the internet—not to mention the many different committees that will be involved in both the House and Senate, and the inevitable need to compromise among them in order for a bill to make it through the entire process—means that you may not recognize your legislative handiwork in the final product. So even though it is possible to imagine that a "perfect" bill might emerge from the Commerce Committee that would clarify and improve Section 230 while preserving all of its benefits, the legislative process that will inevitably follow is likely to adulterate that "perfection" and potentially threaten the essential elements of Section 230 that make it work. This very real risk to the many societal benefits that a majority of Congress still believes flow from Section 230 is worth considering before opening what could be a Pandora's box.

Background and Legislative History of Section 230

Section 230 was signed into law 24 years ago, in 1996.[3] When my colleague Ron Wyden (D–OR) and I conceptualized the law in 1995, roughly 20 million American adults had access to the internet, compared to 7.5 billion today.

Those who were early to take advantage of the opportunity to "surf the web," including many in Congress, quickly confronted this essential aspect of online activity: on each website, many users converge through one portal. The difference between newspapers and magazines, on the one hand, and the World Wide Web (as it was then called), on the other hand, was striking. In the print world, a single staff of human beings reviewed and cataloged editorial content that was then distributed to a large number of passive recipients. The same was true of television and radio. On the web, in contrast, millions of users themselves created content which became accessible to the entire planet immediately. While the volume of users was only in the millions, not the billions as today, it was even then evident to almost every user of the web that no group of human beings would ever be able to keep pace with the growth of content on the internet.

At the time, however, not all in Congress were users of the web who appreciated these fundamentals. The Communications Decency Act ("CDA"), introduced in the Senate by James Exon (D–NE), was premised on the notion that the FBI could filter the web, screening out offensive content. This was a faulty premise based on a fundamental misunderstanding of the scale and the functioning of the internet. Nonetheless, in large part because the stated target of the CDA was pornography, the Senate voted overwhelmingly (the vote was 84–16) in favor of it.[4]

Section 230 was not part of the CDA. Instead, it was a freestanding bill introduced in the House as H.R. 1978, the Internet Freedom and Family Empowerment Act, in June 1995. It was intended as an *alternative* to the CDA. When it was offered as a standalone floor Cox-Wyden amendment during consideration of the Telecommunications Act in August 1995, it was roundly endorsed on both sides of the aisle during debate. At the same time, both Democratic and Republican lawmakers sharply criticized the CDA. They then voted nearly unanimously in favor of the Cox-Wyden amendment, while excluding the CDA from the House version of the Telecommunications Act.

In the conference on what became the Telecommunications Act of 1996 that followed, as is so often the case in legislative compromises between House and Senate, the conferees on agreed to include both diametrically opposed bills in the Conference Report. Subsequently, the U.S. Supreme Court gutted the CDA's indecency provisions, which it found violated the First Amendment, giving Rep. Wyden and me the victory we did not at first achieve in conference.[5]

The fundamental flaw of the CDA was its misunderstanding of the Internet as a medium. We can now easily see that it would have been impossible for the bul-

[3] 104 P.L. 104, 110 Stat. 56.
[4] *Id.*
[5] *Reno v. American Civil Liberties Union,* 521 U.S. 844 (1997).

letin boards, chat rooms, forums, and e-mail that were then budding on the web to be screened in any meaningful way by the FBI, or by the operators of individual websites themselves, even at the far lower volumes of traffic that existed then. Worse, if the law were to demand such screening, the fundamental strength of the new medium—facilitating the free exchange of information among millions of users—would be lost.

*The **Prodigy** and **CompuServe** cases*

The impetus for the Internet Freedom and Family Empowerment Act, today's Section 230, was a New York Superior Court case that I first saw reported in the *Wall Street Journal* in May 1995.[6] It involved one of the leading Internet portals of the day. The case concerned an allegedly defamatory bulletin board post on the Prodigy web service by an unknown user. The post claimed that an investment bank and its founder, Jordan Belfort, had committed securities fraud. (The post was not in fact defamatory: Belfort was later convicted of securities fraud, but not before Prodigy had settled the case for a substantial figure. Belfort would achieve further infamy when he became the model for Leonardo DiCaprio's character in "The Wolf of Wall Street.")

By holding Prodigy liable for the allegedly illegal content posted by its user, the New York court established a new precedent with far-reaching consequences.[7] Up until then, the courts had not permitted such claims for third-party liability. In 1991, a Federal district court in New York held that CompuServe, another web service similar to Prodigy that hosted a variety of user-created content, was not liable in circumstances very similar to those in the *Prodigy* case. The court reasoned that CompuServe "had no opportunity to review the contents of the publication at issue before it was uploaded into CompuServe's computer banks," and therefore was not subject to publisher liability for the third party content.[8]

But in the 1995 New York Superior Court case, the court distinguished the *CompuServe* precedent. The reason the court offered was that unlike CompuServe, Prodigy sought to impose general rules of civility on its message boards and in its forums. While Prodigy had even more users than CompuServe and thus even less ability to screen material on its system, the fact it had announced rules of the road and occasionally enforced them was the judge's basis for subjecting it to liability that CompuServe didn't face.

The perverse incentive this case established was clear: any provider of interactive computer services should avoid even modest efforts to moderate the content on its site. The inevitable consequences for the future of the Internet were equally clear: every website would be incentivized to follow CompuServe's model of "anything goes." Unless corrective action were taken the internet, already beginning to show some erosion in standards of public discourse that must inevitably arise when thousands and then millions of people engage in uninhibited public expression on any topic, would quickly become nothing but a sewer. When I read about this decision, I immediately set to work on drafting a bill to head off its predictable bad consequences.

Creating Section 230 and its goals

The first person I turned to as a legislative partner on my proposed bill was then-Rep. Ron Wyden (D–OR). We had previously agreed to seek out opportunities for bipartisan legislation. As this was a novel question of policy that had not hardened into partisan disagreement (as was too often the case with so many other issues), we knew we could count on a fair consideration of the issues from our colleagues on both sides of the aisle.

For the better part of a year, we conducted outreach and education on the challenging issues involved. In the process, we built not only overwhelming support, but also a much deeper understanding of the unique aspects of the Internet that require clear legal rules for it to function.

The rule established in the Internet Freedom and Family Empowerment Act,[9] which we introduced in June 1995, was crystal clear: the government would impose liability on criminals and tortfeasors for wrongful conduct. It would not shift that liability to third parties, because doing so would directly interfere with the essential functioning of the internet.

---

[6] Milo Geyelin, *New York judge rules Prodigy responsible for on-line content,* Wall St. Jo., May 26, 1995.

[7] *Stratton Oakmont v. Prodigy Servs. Co.,* 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995)

[8] *Cubby, Inc. v. CompuServe, Inc.,* 776 F. Supp. 135, 140 (S.D.N.Y. 1991) (emphasis added).

[9] Internet Freedom and Family Empowerment Act, H.R. 1978, 104 Cong. (1995).

Rep. Wyden and I were well aware that whether a person is involved in criminal or tortious conduct is in every case a question of fact. Simply because one operates a website, for example, does not mean that he or she cannot be involved in lawbreaking. To the contrary, as the last two decades of experience have amply illustrated, the internet—like all other means of telecommunication and transportation—can be and often is used to facilitate illegal activity.

Section 230 was written, therefore, with a clear fact-based test:

- Did the person create the content? If so, that person is liable for any illegality.
- Did someone else create the content? Then that someone else is liable.
- Did the person do anything to develop the content created by another, even if only in part? If so, the person is liable along with the content creator.

The plain language of the statute directly covers the situation in which someone (or some company) is only partly involved in creating the content. Likewise, it covers the situation in which they did not create the content but were, at least in part, responsible for developing it. In both cases, Section 230 comes down hard on the side of law enforcement. A website operator involved only in part in content creation, or only in part in the development of content created by another, is nonetheless treated the same as the content creator.

Here is the precise language of section 230 in this respect:

> The term "information content provider" means any person or entity that is responsible, in whole or *in part,* for the creation *or development of* information provided through the Internet. . . .[10]

These words in Section 230—"in part" and "development of"—are the most important part of the statute. That is because in enacting Section 230, it was not our intent to create immunity for criminal and tortious activity on the internet. To the contrary, our purpose (and that of every legislator who voted for the bill) was to ensure that innocent third parties will not be made liable for unlawful acts committed wholly by others.

If an interactive computer service becomes complicit, in whole or in part, in the creation of illicit content—even if only by partly "developing" the content—then it is entitled to no Section 230 protection.

Rep. Wyden and I knew that, in light of the volume of content that even in 1995 was crossing most Internet platforms, it would be unreasonable for the law to presume that the platform will screen all material. We also well understood the corollary of this principle: if in a specific case a platform actually did review material and edit it, then there would be no basis for assuming otherwise. As a result, the plain language of Section 230 deprives such a platform of immunity.

We then created an exception to this deprivation of immunity, for what we called a "Good Samaritan."[11] If the purpose of one's reviewing content or editing it is to restrict obscene or otherwise objectionable content, then a platform will be protected. Obviously, this exception would not be needed if Section 230 provided immunity to those who only "in part" create or develop content.

The importance of Section 230 for user-generated content

In simplest terms, Section 230 protects website operators that are not involved in content creation from liability for content created by third party users. Without it, websites would be exposed to lawsuits for everything from users' product reviews to book reviews. Yelp would be exposed to lawsuits for its users' negative comments about restaurants, and Tripadvisor could be sued for a user's disparaging review of a hotel. Any service that connects buyers and sellers, workers and employers, content creators and a platform, victims and victims' rights groups—or provides any other interactive engagement opportunity we can imagine—would face open-ended liability if it continued to display user-created content.

How important is user-created content? Without it, it is hard to imagine how any of us would have made it this far through the Covid quarantines and self-isolation of 2020. Many contending with this year's devastating tornadoes—this is already the deadliest tornado season in the United States since 2011—could not have found their loved ones. This year more than ever, millions of Americans are relying on "how to" and educational videos for everything from healthcare to home maintenance. During the Covid crisis, online access to user-created pre-K, primary, and secondary education and lifelong learning resources has proven a godsend for families across the country.

---

[10] 47 USC § 230(f) (emphasis added).

[11] 47 U.S.C. § 230 (c)(2)(A).

Over 85 percent of businesses rely on user-created content on their websites.[12] The vast majority of Americans feel more comfortable buying a product after researching user generated reviews,[13] and over 90 percent of consumers find user-generated content helpful in making their purchasing decisions.[14] User generated content is vital to law enforcement and social services. Following the recent rioting in several U.S. cities, social workers have been able to match people with supplies and services to victims who needed life-saving help, directing them with real-time maps.

Protecting the innocent and punishing the guilty

Throughout the history of the internet, Congress has sought to strike the right balance between opportunity and responsibility. Section 230 is such a balance—holding content creators liable for illegal activity while protecting Internet platforms from liability for content created entirely by others. At the same time, Section 230 does not protect platforms liable when they are complicit—even if only in part ‒ in the creation or development of illegal content.

The plain language of Section 230 makes clear its deference to criminal law. The entirety of Federal criminal law enforcement is unaffected by Section 230. So is all of state law that is consistent with the policy of Section 230.[15]

Still, state law that is inconsistent with the aims of Section 230 is preempted. Why did Congress choose this course? First, and most fundamentally, it is because the essential purpose of Section 230 is to establish a uniform Federal policy, applicable across the internet, that avoids results such as the state court decision in *Prodigy.*[16] The Internet is the quintessential vehicle of interstate, and indeed international, commerce. Its packet-switched architecture makes it uniquely susceptible to multiple sources of conflicting state and local regulation, since even a message from one cubicle to its neighbor inside the same office can be broken up into pieces and routed via servers in different states.

Were every state free to adopt its own policy concerning when an Internet platform will be liable for the criminal or tortious conduct of another, not only would compliance become oppressive, but the Federal policy itself could quickly be undone. All a state would have to do to defeat the Federal policy would be to place platform liability laws in its criminal code. Section 230 would then become a nullity. Congress thus intended Section 230 to establish a uniform Federal policy, but one that is entirely consistent with robust enforcement of state criminal and civil law.

Despite the necessary preemption of inconsistent state laws, every state and every Federal prosecutor can successfully target online criminal activity by properly pleading that the defendant was at least partially involved in the creation of illegal content, or at least the later development of it. In all such cases, Section 230 immunity does not apply.

How Section 230 actually works

The importance to millions of Americans of so many topics that Section 230 touches upon either directly or indirectly—for example, the responsibility of social media platforms to their users and the public; the ability of citizens to exercise their First Amendment rights; the ability of law enforcement to track down criminals; the protection of the privacy of every user of the internet—means that almost everyone has an opinion about Section 230 itself. But notwithstanding that Section 230 has become a household name, a complete understanding of how the law functions in practice, and what it actually does, is harder to come by. There are several misconceptions abroad that merit clarification.

Some mistakenly claim that Section 230 prevents action against websites that knowingly engage in, solicit, or support illegal activity. This is simply wrong. But since this claim is often a principal basis for urging amendment of Section 230, it bears repeating that Section 230 provides no protection for any website, user, or other person or business involved *even in part* in the creation *or development* of content that is tortious or criminal.

In the two and a half decades that Section 230 has been on the books, there have been hundreds of court decisions interpreting and applying it. It is now firmly established in the case law that Section 230 cannot act as a shield whenever a website

---

[12] *https://www.semrush.com/blog/50-stats-about-9-emerging-content-marketing-trends-for-2016/*

[13] Wu, Y. (2015). What Are Some Interesting Statistics About Online Consumer Reviews? Dr4ward.com. Available at: *http://www.dr4ward.com/dr4ward/2013/03/what-are-some-interesting-statistics-about-online-consumer-reviews-infographic.html*

[14] Kimberly Morrison, "Why Consumers Share User-Generated Content," *Adweek,* May 17, 2016.

[15] 47 USC § 230(e)(3).

[16] *Stratton Oakmont v. Prodigy Servs. Co.,* 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995).

is in any way complicit in the creation or development of illegal content. In the landmark *en banc* decision of the Ninth Circuit Court of Appeals in *Fair Housing Council of San Fernando Valley v. Roommate.com,*[17] which has since been widely cited and applied across the United States, it was held that not only do websites lose their immunity when they merely "develop" content created by others, but participation in others' content creation can be established by the wholly automated features of a website that are coded into its architecture.

There are many examples of courts faithfully applying the plain language of Section 230 to hold websites liable for complicity in the creation or development of illegal third-party content. In its 2016 decision in *Federal Trade Comm'n v. Leadclick Media, LLC,*[18] the Second Circuit Court of Appeals rejected a claim of Section 230 immunity by an Internet marketer even though it did not create the illegal content at issue, and the content did not appear on its website. The court noted while this was so, the Internet marketer gave advice to the content creators. This made it complicit in the development of the illegal content, and so ineligible for Section 230 immunity.

In *FTC v. Accusearch,*[19] the Tenth Circuit Court of Appeals held that a website's mere posting of content that it had no role whatsoever in creating—telephone records of private individuals—constituted "development" of that information, and so deprived it of Section 230 immunity. Even though the content was wholly created by others, the website knowingly transformed what had previously been private information into a publicly available commodity. Such complicity in illegality was deemed to constitute "development" of the illegal content, as distinguished from its creation.

Other notable examples of this now well-established feature of Section 230 are *Enigma Software Group v. Bleeping Computer,*[20] in which a website was denied immunity despite the fact it did not create the unlawful content at issue, because of an implied agency relationship with an unpaid volunteer who did create it; and *Alvi Armani Medical, Inc. v. Hennessey,*[21] in which the court deemed a website to be complicit in content creation because of its alleged knowledge that postings were being made under false identities.

In its 2016 decision in *Jane Doe v. Backpage.com,*[22] however, the First Circuit Court of Appeals cast itself as an outlier, rejecting the holding in *Roommate.com* and its progeny. Instead, it held that "claims that a website facilitates illegal conduct through its posting rules *necessarily* treat the website as a publisher or speaker of content provided by third parties and, thus, are precluded by section 230(c)(1)."[23] This holding completely ignored the definition in subsection (f)(3) of Section 230, which provides that anyone—including a website—can be an "information content provider" if they are "responsible, in whole or in part, for the creation or development" of online content. If a website's posting rules facilitate the development of illegal content, then the website becomes a content provider in its own right, and should be deprived of Section 230 immunity.

Despite the fact that the First Circuit was an outlier in this respect, the notoriety of its decision in the *Backpage* case has given rise to the notion that Section 230 routinely operates as a shield against actual wrongdoing by websites. The opposite is the case. Courts since 2016 have consistently followed the *Roommate* precedent, and increasingly have expanded the circumstances in which they are willing to find websites complicit in the creation or development of illegal content provided by their users.

Ironically, the actual facts in the *Backpage* case were a Technicolor display of complicity in the development of illegal content. Backpage knowingly concealed evidence of criminality by systematically editing its adult ads; it coached its users on how to post "clean" ads for illegal transactions; it deliberately edited ads in order to facilitate prostitution; it prescribed the language used in ads for prostitution; and it moderated content on the site, not for the purpose of removing ads for prostitution, but to camouflage them. It is difficult to imagine a clearer case of complicity "in part, for the creation or development" of illegal content.

---

[17] 521 F.3d 1157, 1168 (9th Cir. 2008).
[18] 838 F.3d 158 (2d Cir. 2016).
[19] 570 F.3d1187, 1197 (10th Cir. 2009).
[20] 194 F.Supp.3d 263 (2016).
[21] 629 F. Supp. 2d 1302 (S.D. Fla. 2008).
[22] *Jane Doe No. 1, et al., v. Backpage.com LLC, et al.,* No. 15–1724 (1st Cir. 2016).
[23] *Id.* (emphasis added).

Happily, even within the First Circuit, this mistake has now been rectified. In the 2018 decision in *Doe v. Backpage.com,*[24] a re-pleading of the original claims by three new Jane Doe plaintiffs, the court held that allegations that Backpage changed the wording of third-party advertisements on its site were sufficient to deem it an information content provider, and thus ineligible for Section 230 immunity. Much heartache could have been avoided had these allegations concerning Backpage's complicity been sufficiently pleaded in the original case,[25] and had the court reached this sensible and clearly correct decision on the law in the first place.

Another misguided notion is that Section 230 was never meant to apply to e-commerce. To the contrary, removing the threat to e-commerce represented by the *Prodigy* decision was an essential purpose in the development and enactment of Section 230.

When Section 230 became law in 1996, user-generated content was already ubiquitous on the internet. The creativity being demonstrated by websites and users alike made it clear that online shopping was an enormously consumer-friendly use of the new technology. Features such as CompuServe's "electronic mall" and Prodigy's mail-order stores were instantly popular. So too were messaging and e-mail, which in Prodigy's case came with per-message transaction fees. Web businesses such as CheckFree demonstrated as far back as 1996 that online bill payment was not only feasible but convenient. Prodigy, America Online, and the fledgling Microsoft Network included features we know today as content delivery, each with a different payment system.

Both Rep. Wyden and I had all of these iterations of Internet commerce in mind when we drafted our legislation. We made this plain during floor debate.[26]

Yet another misconception about the coverage of Section 230, often heard, is that it created one rule for online activity and a different rule for the same activity conducted offline. To the contrary, Section 230 operates to ensure that like activities are always treated alike under the law.

When Section 230 was written, just as now, each of the commercial applications flourishing online had an analog in the offline world, where each had its own attendant legal responsibilities. Newspapers could be liable for defamation. Banks and brokers could be held responsible for failing to know their customers. Advertisers were responsible under the Federal Trade Commission Act and state consumer laws for ensuring their content was not deceptive and unfair. Merchandisers could be held liable for neg-ligence and breach of warranty, and in some cases even subjected to strict liability for defective products.

In writing Section 230, Rep. Wyden and I, and ultimately the entire Congress, decided that these legal rules should continue to apply on the Internet just as in the offline world. Every business, whether operating through its online facility or through a brick-and-mortar facility, would continue to be responsible for all of its legal obligations. What Section 230 added to the general body of law was the principle that an individual or entity operating a website should not, in addition to its own legal responsibilities, be required to monitor all of the content created by third parties and thereby become derivatively liable for the illegal acts of others. Congress recognized that to require otherwise would jeopardize the quintessential function of the internet: permitting millions of people around the world to communicate simultaneously and instantaneously. Congress wished to "embrace" and "welcome" this not only for its commercial potential but also for "the opportunity for education and political discourse that it offers for all of us."[27]

The result is that websites are protected from liability for user-created content, but *only if they are wholly uninvolved in the creation or development of that content.* Today, virtually every brick-and-mortar business of any kind, from newspapers to retailers to manufacturers to service providers, has an Internet presence through which it conducts e-commerce. Whether in the offline world or the internet, the same legal rules and responsibilities apply across the board to all.

It is worth debunking three other "creation myths" about Section 230.

The first is that Section 230 was conceived as a way to protect an infant industry. According to this narrative, in the early days of the internet, Congress decided that

---

[24] *Doe No. 1 v. Backpage,* 2018 WL 1542056 (D. Mass. March 29, 2018).

[25] Although the plaintiffs disputed this, in the original case the First Circuit pointedly noted that the record before it expressly *did not* allege that Backpage contributed to the development of the sex trafficking content, even "in part." Instead, the argument that Backpage was an "information content provider" under Section 230 was "forsworn" in the district court and on appeal.

[26] S*ee* 141 Cong. Rec. H8468–72, H8478–79 (August 4, 1995).

[27] Id. at H8470.

small startups needed protection. Now that the Internet has matured, it is argued, the need for such protection no longer exists; Section 230 is no longer necessary.

As co-author of the legislation, I can verify that this is an entirely fictitious narrative. Far from wishing to offer protection to an infant industry, our legislative aim was to recognize the sheer implausibility of requiring each website to monitor all of the user-created content that crossed its portal each day. In the 1990s, when Internet traffic was measured in the tens of millions, this problem was already apparent. Today, in the second decade of the 21st century, the enormous growth in the volume of traffic on websites has made the potential consequences of publisher liability far graver. Section 230 is needed for this purpose now, more than ever.

The second "creation myth" is that Section 230 was adopted as a special favor to the tech industry, which lobbied for it on Capitol Hill and managed to wheedle it out of Congress by working the system. The reality is far different. In the mid-1990s, Internet commerce had very little presence in Washington. When I was moved to draft legislation to remedy the *Prodigy* decision, it was based on my reading news reports of the decision. No company or lobbyist contacted me. Throughout the process, Rep. Wyden and I heard barely at all from the leading Internet services of the day. This included both Prodigy and CompuServe, whose lawsuits inspired the legislation. As a result, our discussions of the proposed legislation with our colleagues in the House and Senate were unburdened by importunities from businesses seeking to gain a regulatory advantage over their competitors.

I willingly concede that this was, therefore, a unique experience in my lawmaking career. It is also the opposite of what Congress should expect if it undertakes to amend Section 230, given that today millions of websites and more millions of Internet users have an identifiable stake in the outcome.

The final creation myth is that Section 230 was part of a grand bargain with Senator James Exon (D–NE), in which his Communications Decency Act aimed at pornography was paired with the Cox-Wyden bill, the Internet Freedom and Family Empowerment Act, aimed at greenlighting websites to enforce content moderation policies without fear of liability. The claim now being made is that the two bills were actually like legislative epoxy, with one part requiring the other. And since the Exon legislation was subsequently invalidated as unconstitutional by the U.S. Supreme Court, so the argument goes, Section 230 should not be allowed to stand on its own.

In fact, the revisionists contend, the primary congressional purpose back in 1996 was not to give Internet platforms limited immunity from liability as Section 230 does. Rather, the most important part of the imagined "package" was Senator Exon's radical idea of imposing stringent liability on websites for the illegal acts of others—an idea that Exon himself backed away from before his amendment was actually passed. Now, a quarter-century after the Supreme Court threw out the Exon bathwater, the neo-speech regulators are urging us to throw out the Section 230 baby along with it.

The reality is far different than this revisionist history would have it. In fact, the Cox-Wyden bill was deliberately crafted as a rebuke of the Exon approach. When it came to the House floor for consideration, speaker after speaker rose to speak in support, and at the same time criticized the Exon approach. Rep. Zoe Lofgren (D–CA), the mother of 10- and 13-year-old children, shared her concerns with Internet pornography and noted that she had sponsored legislation mandating a life sentence for the creators of child pornography. But, she emphasized, "Senator Exon's approach is not the right way. . . . It will not work." It was, she said, "a misunderstanding of the technology."

Rep. Bob Goodlatte, a Virginia Republican, emphasized the potential the Internet offered and the threat to that potential from Exon-style regulation. "We have the opportunity for every household in America, every family in America, soon to be able to have access to places like the Library of Congress, to have access to other major libraries of the world, universities, major publishers of information, news sources. There is no way," he said, "that any of those entities, like Prodigy, can take the responsibility to edit out information that is going to be coming in to them from all manner of sources."

In the end, not a single representative spoke against the bill. The final roll call on the Cox-Wyden amendment was 420 yeas to 4 nays. It was a resounding rebuke to the Exon approach in his Communications Decency Act. The House then proceeded to pass its version of the Telecommunications Act—with the Cox-Wyden amendment, and without Exon.

When the House and Senate met in conference on the Telecommunications Act, the House conferees sought to include Cox-Wyden and strike Exon. But political realities as well as policy details had to be dealt with. There was the sticky problem of 84 senators having already voted in favor of the Exon amendment. Once on

record with a vote one way—particularly a highly visible vote on the politically charged issue of pornography—it would be very difficult for a politician to explain walking it back. The Senate negotiators, anxious to protect their colleagues from being accused of taking both sides of the question, stood firm. They were willing to accept Cox-Wyden, but Exon would have to be included, too. The House negotiators, all politicians themselves, understood. This was a Senate-only issue, which could be easily resolved by including both amendments in the final product. It was logrolling at its best.

Perhaps part of the enduring confusion about the relationship of Section 230 to Senator Exon's legislation has arisen from the fact that when legislative staff prepared the House-Senate conference report on the final Telecommunications Act, they grouped both Exon's Communications Decency Act and the Internet Freedom and Family Empowerment Act into the same legislative title. So the Cox-Wyden amendment became Section 230 of the Communications Decency Act—the very piece of legislation it was designed to counter. Ironically, now that the original CDA has been invalidated, it is Ron's and my legislative handiwork that forever bears Senator Exon's label.

Measuring the PACT Act and Other Pending Federal Legislation Against the Goals Section 230 Is Meant to Achieve

When Congress enacted what we know today as Section 230 by near-unanimous votes in the House and the Senate, there was broad agreement on several basic principles. Some of these are set forth in the law's preamble; others are set forth in the operational portion of the statute. These basic tenets are as follows:

- The wide array of interactive educational and informational services available to individual Americans via the Internet represents an extraordinary resource worth preserving.
- The ideal way to control the flow of information on the internet, and to screen wanted from unwanted information, is not for government to regulate that flow, but rather for each individual user to have the greatest possible control over what they receive.
- The fact that the Internet is not centrally controlled and regulated, but largely comprised of content created by millions of individual users, makes it a global forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
- The Internet has flourished, to the benefit of all Americans who rely upon it for a variety of political, educational, cultural, and entertainment services, with a minimum of government regulation.
- Content moderation aimed at keeping websites free from obscenity, stalking, harassment, terrorism, criminal activity, and other objectionable content and behavior should not be penalized by exposing those websites who undertake it to increased liability for their efforts.

Twenty-four years later, while the Internet itself has changed in many ways, these fundamental principles remain sound. The task for 21st century lawmakers is to determine whether these goals are being achieved, and to explore ways to address any shortcomings. Remedial legislation, if it is found warranted, should seek to preserve and extend the benefits that Congress overwhelmingly agreed can and should be forthcoming from the internet. Accordingly, any new bill with the goal of updating Section 230 or related areas of Federal law should be measured against this template.

In the current Congress, a number of bills have been introduced in both chambers dealing directly or indirectly with content moderation. These include S. 3398, the EARN IT Act; S. 1914, the Ending Support for Internet Censorship Act; H. R. 4027, the Stop the Censorship Act; S. 3983, the Limiting Section 230 Immunity to Good Samaritans Act; and S.4062, Stopping Big Tech's Censorship Act. In this committee, you are considering the Platform Accountability and Consumer Transparency Act (PACT Act), which is aimed at increasing transparency of content moderation policies and ensuring that knowing participation in criminal activity is punishable to the full extent of the law. These are worthy objectives and I commend the committee for prioritizing them.

PACT Act

Considering the PACT Act in light of the original purposes of Section 230, I offer the following observations.

First, the PACT Act itself embraces the important policy objectives set out in the original Section 230. It repeats Section 230's intention to preserve and encourage

the continued technological advancement of the internet, in recognition of the substantial benefits the Internet provides both to consumers and to the overall economy. The bill also highlights the fact that people throughout the United States rely on the Internet for a wide variety of things, including communicating with friends and loved ones as well as the wider world; gathering information from others and broadcasting their own creations; and conducting commercial transactions of endless variety.

Plainly, the purpose of these declarations in the PACT Act is to set out an overarching objective of ensuring that these benefits aren't comprised. This is an aspiration I wholeheartedly endorse. It is also a useful standard against which to measure the operational portions of the bill.

Finally, the preamble to the PACT Act declares that free expression is an essential feature of the Internet that should be protected. The bill recognizes that the Internet is a uniquely successful facilitator of communications now essential to economic, political, social, and cultural life in America and around the world. This essential characteristic of the internet, which arises from its decentralized architecture that permits millions (indeed billions) of users to interact in real time, was of great importance to me and to the other members of Congress in the mid-1990s when we enacted Section 230. In this respect, the PACT Act and Section 230, at least insofar as their ultimate aims, are aligned.

The bill is divided into three main parts, dealing with transparency, liability, and enforcement. I will address each one in order. Before doing so, I should note several things the bill doesn't do. In each case, in my judgment, the decision of the PACT Act authors to avoid going down these paths reflects the better part of wisdom.

Encryption: The bill eschews the approach of the original version of the EARN IT bill, which had the potential to compromise existing consumer privacy protections by raising the possibility that encryption designed to be secure against everyone except the user who holds the key might expose platforms to new liability. It is a noble legislative aim to incentivize creation of a technically feasible means of "lawful access" that only the government could exploit, but cybersecurity is a constant game of cat-and-mouse in which bad actors are constantly outwitting the latest protections. Despite best efforts, the U.S. government has been hacked many times, and millions of people have lost sensitive information as a result, including not only their Social Security numbers but also detailed private information about their law enforcement, medical, financial, and employment records containing such highly protected data as fingerprints and mental health diagnoses, as well as equally personal information on children and other family members. The Pentagon, the SEC, HHS, the Executive Office of the President, and several member departments and agencies within the intelligence community have been penetrated.

In many cases these successful exploits of U.S. government security have been accomplished by sophisticated foreign actors with state sponsorship.

Congress most certainly should be examining how law enforcement aims can be achieved in tandem with rigorous protection of individual Americans' privacy. But leaping into that morass with mandates or penalties that require the creation of "backdoors," before the technology exists to guarantee that the backdoors will not themselves become the means of illegal exploitation, is premature.

Political Neutrality: As distinct from S. 1914 and S. 4062, the PACT Act does not condition Section 230 protections for websites hosting user-created content on their being "politically neutral." Ensuring that the Internet remains "a global forum for a true diversity of political discourse" requires that government allow a thousand flowers to bloom—not that a single website has to represent every conceivable point of view. Section 230 does not require political neutrality, and was never intended to do so. Were it otherwise, to use an obvious example, neither the Democratic National Committee nor the Republican National Committee websites would pass a political neutrality test. Government-compelled speech is not the way to ensure diverse viewpoints. Permitting websites to choose their own viewpoints is.

Websites that choose to be politically neutral, and hold themselves out as such, can be held to this standard. When an Internet platform promises its customers—through its advertising, published community standards, and terms of service—that its content moderation policy is politically neutral, then that promise can be enforced both by the government and civil litigants under existing Federal and state laws. This is far different than a mandate of political neutrality, with the judgment of what is and is not "neutral" placed in the hands of political appointees in Washington. The PACT Act wisely shuns this approach.

Subjective Standards: Several commentators have urged grafting onto Section 230 a requirement, derived from negligence law, upon which existing protections for content moderation would be conditioned. Typically taking the form of a "duty of care" or a "reasonableness" standard, the proposals would effectively make every com-

plaint that a website has failed to meet the standard into a question of fact. Since such fact disputes can only be resolved after evidentiary discovery (depositions of witnesses, written interrogatories, subpoenas of documents, and so forth), no longer could a website prove itself eligible for dismissal of a case at an early stage. An essential feature of Section 230 is its objective standard: was the allegedly illegal material created or developed—in whole or in part—by the website? If the complaint adequately alleges this, then the website can be treated as a publisher and held liable for the material; otherwise not.

Without an objective standard to determine whether lawsuits can proceed, a website would constantly be exposed to open-ended, multi-year litigation over any or all of the user-created content it hosts. The defining characteristic of the internet—the convergence of many (frequently millions and occasionally billions) of users on a single platform—means that a website would have no way to protect itself from a multiplicity of such lawsuits, short of scaling back or eliminating user-created content. Currently, civil suits in the Federal system that proceed beyond a motion to dismiss on the pleadings last an average of three years through trial; appeals can consume years more. For this reason, over 90 percent of cases settle without a judge or jury actually applying the law to the facts in their case. The mere filing of a lawsuit in such circumstances can create significant settlement value for a plaintiff. The fact that a typical website could easily face hundreds or even thousands of such suits illustrates the severity of the threat to the functioning of the Internet itself.

The PACT Act does not seek to graft subjective negligence-type concepts such as a duty of care onto the currently objective criteria in Section 230. Because ensuring that Section 230 can be applied by courts at the motion to dismiss stage is essential to achieving its purposes, this is an important conceptual pitfall for any remedial legislation to avoid.

Monitoring User-Created Content: Essential to the functioning of the internet, and to reaping the benefits of its characteristic feature of real-time communication among unlimited numbers of users, is that websites hosting content do not have to monitor every piece of content. The sheer volume of communications arising from a planetary base of potential users makes this an unreasonable requirement. Even if a website could somehow staff up to meet this near-impossible burden, doing so would ensure that Internet communications via that platform could not proceed in real time. Nonetheless, several legislative proposals would impose potential legal liability on websites that could only be avoided by constant monitoring of all user-created content. This is a situation that Section 230 was intended to prevent. The PACT Act wisely avoids the imposition of a monitoring requirement, and indeed contains language in section 5 stating that monitoring or "affirmative fact-seeking" is not required in connection with complaints received. (A similar disclaimer should be added to the bill to clarify that such an obligation does not exist in any case, whether in connection with a complaint or not.)

Takedown Based on Private Accusations: Several commentators have recommended that U.S. law be amended to require, following the model of the Digital Millennium Copyright Act, the mandatory takedown of content once a website has been notified that it is defamatory or otherwise violative of law. Such a requirement would empower anyone willing to allege defamation to require the immediate removal of speech with which they disagree. The PACT Act avoids this pitfall. Instead, its requirement of mandatory takedown of illegal content and conduct applies only when that content or conduct has been determined by a court to be violative of law. While there are other issues created by the language in the bill as drafted, the legislative choice not to create opportunities for the exercise of a "heckler's veto" is the correct one.

Internet Infrastructure Services: Section 230 defines the term "interactive computer service" broadly, because it was intended that the law's protections extend broadly to ensure that content moderation and free expression would be protected. If Congress decides to use Section 230 as a vehicle for placing new burdens and liabilities on web platforms, care should be taken to distinguish between them and the Internet infrastructure providers that are swept within the broad definition of "interactive computer service." For example, DNS registries do not operate content publishing platforms and indeed have no direct relationships with end users of the internet. As infrastructure providers, they are very different from social media platforms and search engines. The PACT Act does not attempt to regulate Internet infrastructure providers, and indeed the bill includes language forswearing this with respect to web hosting, domain registration, content delivery networks, caching, back-end data storage, and cloud management. This distinction between websites and Internet infrastructure providers is an important one to make.

Turning now to the PACT Act's three main sections, and taking them in order, I offer the following comments and suggestions.

Transparency

Transparency—meaning disclosure to consumers, regulators, stakeholders, and the public generally of how a platform moderates content—is a sound objective. The PACT Act's prioritization of transparency is unquestionably constructive and consistent with Section 230 and its ultimate aims.

The mechanisms through which the bill would promote transparency include statutory standards for each website's content moderation policy; mandatory complaint systems for each website that include toll-free call-in services and web-based mechanisms, to be used when websites fail to meet the content moderation standards; required notice and hearing, including a right to appeal, for each complaint received; and mandatory recordkeeping and reporting of content moderation decisions and disposition of complaints. In addition, the Federal Trade Commission is given authority to enforce the statutory standards and the content moderation policies of every website.

While overall these provisions could be made to be workable, as drafted they will run afoul of the objectives of Section 230 and threaten the smooth functioning of the Internet and the currently robust environment for user-created content.

'Potentially policy-violating content': Specifically, section 5 of the bill includes in its mandates for an "acceptable use policy" the requirement that websites provide due process notices, hearings, and appeals in response to every complaint that third-party content "potentially" violates the website's community standards. There are three problems with this approach.

First, the website's own standards may or may not be admirable from a public policy perspective. Given that—so long as the statutory requirements concerning illegal content and activity are met—websites are free to adopt whatever content policies they wish, it is reasonable to assume that some websites will welcome content that, while legal, the government would not wish to promote. Any government-mandated complaint system should therefore be focused not on the purely voluntary and idiosyncratic aspects of each website's content policies, but rather on illegal content and illegal activity. This would amply cover not only criminal conduct and content involving sex trafficking, child sexual abuse material, terrorism, illegal drug dealing, stalking, and so forth, but also the wide range of Federal and state civil offenses including defamation and invasion of privacy.

Second, the bill's extension of its due process mandate to cover not only *actual* violations of each website's policy, but also *potential* violations, introduces a subjective concept that will be easily abused. Currently, Section 230 permits a court in most cases to judge whether or not the law applies at an early stage, based on the pleadings. This ensures that the mere lodging of a complaint does not trigger elaborate expense for the website—particularly important given the volume of user-created content often handled by even the smallest websites. By reducing what must be alleged in a telephone or e-mail complaint to the mere possibility that content or activity could *potentially* violate the website's policy, the PACT Act as written would make it trivially easy for anyone to trigger the notice-and-hearing requirements contained in section 5.

Third, the imposition of such a broad notice-and-hearing requirement, which would apply in almost every case given the lax and subjective standard for triggering it, will expose websites to significant expense. (Combined with the high volume of hearings and appeals the bill's subjective standard will generate, its requirement that every complaint be initially researched, analyzed, and disposed of within 14 days will make compliance still more expensive.) Websites will naturally seek to avoid or at least minimize this greater expense.

If almost every complaint requires a hearing and triggers notice requirements and guarantees an appeal, then the only way to minimize the associated expense will be to reduce the grounds for complaints to be filed. Since every website will have control over the specifics of its content moderation policy, the incentive will be to minimize the number of moderation decisions required, through the adoption of less-robust moderation policies. Alternatively, websites could reduce or eliminate user-created content. Section 230, on the other hand, is intended to protect and encourage content moderation, and to facilitate users' ability to publish their content on the internet. In these ways, the inclusion of allegedly "potentially policy-violating content" as a trigger for mandatory hearings and appeals is at odds with the stated goals of Section 230 and the PACT Act itself.

To better align section 5 with the PACT Act's own stated objectives, therefore, it should be amended to eliminate "potentially policy-violating content" wherever it appears. In addition to remedying the problems noted, this would also conform section 5 with the intermediary liability provisions in section 6, which are focused on illegal content and activity, and not on "potentially policy-violating content."

Data collection and reporting: The specific requirements for data collection and quarterly public reporting based thereon, as set forth in section 5 of the bill, include the following:

1. The number of user complaints about specific content
2. The number of employee flags about specific content
3. The number of contractor flags about specific content
4. The number of internal automated flags about specific content
5. The number of government flags about specific content
6. The number of flags about specific content from other service providers
7. The number of flags from outside personnel employed or contracted by other service providers
8. The country of each provider of content that is subject to a complaint or flag
9. The number of times each specific rule within the website's content policy was violated
10. The number of times the website took one of the following actions with respect to content:
    a) content removal
    b) content demonetization
    c) content deprioritization
    d) appending content with an assessment
    e) account suspension
    f) account removal
11. The number of appeals of decisions on complaints about specific content
12. The number of appeals that resulted in restoration of content previously removed
13. Each mechanism used to enforce the website's content policy, including:
    a) Software and hardware tools
    b) General practices
    c) Specific actions
    d) Proprietary techniques[28]

This ongoing data collection burden would be placed on every website in America with an average daily number of visitors of more than 33,333 and $12 million in annual revenue, thereby sweeping in thousands of small businesses that would have to comply.[29] As onerous as the data collection and reporting could be for such websites, the burden would grow exponentially with the size of the platform. The largest social media platforms, Facebook, Twitter, and Yahoo, remove about three billion posts and accounts every 90 days. The number of "deprioritization" decisions, given the daily and even moment-to-moment automated adjustments that would be encompassed within that rubric, would be far higher. The requirement to maintain detailed recordkeeping for all of this for every individual piece of content, which would then become the basis for public reports that would have to be scrubbed for accuracy before publication, would impose a daunting logistical and economic tax on all but the smallest websites.

The disincentives to do content monitoring at all that would accompany these costly impositions would pose a genuine threat to the goals that both Section 230, and ostensibly the PACT Act itself, are aimed at achieving.

Beyond the sheer burden of compliance with this extensive mandate, the language in the bill poses interpretive challenges. None of the terms used in the long list of categories to be tracked is defined. While "content demonetization" has some meaning in common parlance as it relates to Google, for the 875 million other websites in America that is likely not the case. The same can be said for "content deprioritization." Depending upon the website's particular business model, the term might have no application at all; alternatively, each website might be left to define

---

[28] There is an additional requirement that websites report their actions with respect to questionable content, categorized by "coordinated campaign, if applicable." *See* section 5(d)(2)(B)(iv) of the bill. It is not at all clear what this means.

[29] This is a very low threshold. By comparison, the Small Business Association defines a small business as one with less than $35 million in annual revenue. *See* 13 CFR § 121.201. The PACT Act's implicit definition of a "large" business would sweep in websites one-third the size of what the SBA considers to be a small business.

the term for themselves, with endless different variations on the theme. The lack of rigor in drafting this section of the bill would make compliance, already destined to be expensive and burdensome, needlessly more so.

Liability

The PACT Act would amend Section 230 to deny the law's protection to any website that fails to "remove . . . illegal content or stop illegal activity" within 24 hours of "acquiring . . . knowledge" of it.

It is clear what is intended here. Conduct and content that are in and of themselves illegal should be kept off of all websites subject to the jurisdiction of the United States. That is an unassailable objective. It is also perfectly consistent with the congressional purposes in enacting Section 230 in the first place. Section 230 was never intended to provide a shield for illegal activity.

Notwithstanding the authors' clear purpose, the actual language in section 6 of the bill creates needless ambiguity that will frustrate achievement of that purpose. Happily, sturdier language in the same section of the bill can be used to clarify some of this unintended ambiguity.

The first drafting problem inheres in the bill's reliance on "knowledge" as the trigger for the 24-hour takedown deadline. "Knowledge" is a subjective standard that requires an assessment of state of mind. "Notice" is an objective standard, which if substituted for "knowledge" in this context would eliminate any subjectivity and at the same time fully achieve the authors' objective. The bill attempts to undo its own use of the subjective term by defining "knowledge" to mean "notice." This creates needless interpretive risk. Since section 6 of the bill already contains a detailed definition of "notice" that amply serves the purpose, all that is needed is to change the proposed amendment to Section 230 to require that the website "has notice of the illegal content or illegal activity, as provided in subparagraph (B)."

The second drafting problem concerns the loose description of what the notice must contain by way of identifying specific illegal content. The bill states only that the notice must contain "information reasonably sufficient" to locate the content. Failing to include specific, clear minimum requirements that will in each case guarantee that the website will be able to locate the offending material virtually guarantees that disputes will arise. Clarity in this respect is particularly important given the very short 24-hour deadline for compliance. (Indeed, as millions of websites are not staffed 24/7 or on weekends, that deadline will in many cases be unrealistic.)

The third drafting problem is the definition of "illegal." The bill defines "illegal" content and activity to be that which a court has "determined to violate Federal law or state defamation law." While tightly circumscribing mandatory takedowns to court-adjudicated cases is a wise legislative choice, more clarity is required here to specify what constitutes a court determination. Must it be a final judgment? Must it await the expiration of appeals? And whichever definition is adopted, what is the rationale? These are questions the bill's authors must directly confront and resolve. From the standpoint of websites that will have to comply with this short-fuse takedown requirement, clarity is more important than the particular answer Congress might settle upon.

From the standpoint of policy makers in Congress, however, which answer you choose is indeed important. Consider that many individuals hostile to others' speech are litigious. The automatic operation of this provision of the PACT Act—mandatory takedown after 24 hours' notice—means that it will be a sure-fire way to suppress speech on the internet. In the case of speech involving important public policy issues, by way of example, should a lower court victory be enough? And what of default judgments, where by definition the arguments on the other side have not been fully considered? What of the deliberate falsification of court orders? (The bill contains no sanction for such activity.) Careful weighing of the tradeoffs here will be necessary to ensure that the objectives of protecting free expression and eliminating illegality from the Internet are simultaneously vindicated.

Enforcement

Section 230 was drafted with the intention of protecting the innocent from being held liable for wrongs committed by others. It was equally intended to ensure that those who actually commit wrongs will be subject to prosecution by both civil and criminal law enforcement. One need not rely on the legislative history or the words of the authors for this proposition. The language of the statute is plain enough. If a website, or anyone who provides what the law describes as interactive computer services, is complicit in the creation of unlawful content then it may not claim protection under Section 230. The PACT Act would undo this arrangement. Instead, Section 230 would be waived entirely whenever the Federal government or a state

attorney general is the litigant. In every such case, websites would lose the protection offered by Section 230.

The only conceivable justification for depriving every website of their existing protection under Federal law in this way is that state attorney generals and Federal prosecutors are presumed always to be right, and websites in such cases are presumed always to be wrong. If so, one wonders why a trial would ever be necessary. In my experience as head of a Federal agency charged with civil law enforcement, the agency was—in the judgment of the courts—more often right than wrong, but hardly infallible. A number of Federal departments and agencies in recent years, including the Department of Justice, have been chastised by courts for violating ethical norms in the cases they bring and in the way they have prosecuted them. State attorneys general are all elected political figures involved in political fundraising that frequently presents conflicts of interest. A blanket presumption that the government is always right is too slender a reed on which to rest an across-the-board statutory repeal of Section 230's essential provisions.

There is no reason that Federal and state prosecutors cannot enforce all of their laws without need of such a wholesale waiver of Section 230. Indeed, Section 230 itself states that "Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section." So unless flatout rejection of the very purpose of Section 230 is the objective, the PACT Act should not follow this course. Rather than the blunderbuss approach of simply waiving away the entirety of Section 230 for government litigants, it would be far wiser to more fully accommodate state law enforcement interests through an express statutory authorization to state attorneys general to enforce not only state laws consistent with Section 230, but Federal laws as well. This would multiply the potential for enforcement actions to keep illegal content off of the internet.

Such an authorization could be modeled on the existing provision in 28 U.S.C. § 543 empowering the Department of Justice to appoint participating state Attorneys General as "Special Attorneys." This authority of the Attorney General to appoint "Special Attorneys" dates to 1966. (The statutory authority was most recently amended in 2010.) The internal Department of Justice authority appears in the United States Attorneys Manual (USAM) at USAM § 3–2–200. The authority is very broad, and the terms of the appointment are entirely negotiable. In this way, every state Attorney General who wishes to do so could exercise the full authority not only of his or her state law, but also Federal law. As Section 230 has no application to Federal criminal law, any theoretical arguments about its application to a given state prosecution will immediately evaporate.

S. 3398, EARN IT

The most recent version of the EARN IT bill was reported from the Senate Judiciary Committee on July 20. As amended in committee, the bill would make several changes to Federal law affecting Section 230 and content moderation. The amended bill, like its predecessor, continues to present several serious issues, including constitutional infirmities that could create opportunities for child abusers to escape justice by demanding that the most damning evidence be excluded from their trials.

The bill would mandate the establishment of Federal standards, referred to in the bill as "best practices," that would cover, among other things, the following specific ways that websites and Internet infrastructure providers should be involved in content moderation. While the bill's focus is content related to child sexual exploitation, the "best practices" would necessarily extend to all content prior to its screening and identification as child sexual exploitation material. The Federal standards to be promulgated would include requirements for websites and Internet infrastructure providers to:

1. Preserve on their servers specified user-created content
2. Take down specified user-created content
3. Report to law enforcement and others specified user-created content
4. Record and preserve location data for users
5. Record and preserve other personal identifiable information concerning users
6. Develop and maintain an online service for accepting reports from the public concerning specified user-created content
7. Develop and maintain an internal system for sorting, prioritizing, and allocating resources to complaints and reports received through the online public reporting system
8. Implement a "standard rating and categorization system" to identify specified types of user-created content

9. Train content moderators according to the Federal standards to be promulgated
10. Provide certain specified levels of support to content moderators devoted to searching for online child sexual exploitation material
11. Produce reports to the government covering:
    a) the entity's policies and procedures for "identifying, categorizing, and reporting" online child sexual exploitation
    b) the entity's efforts "to prevent and disrupt" online child sexual exploitation
12. Coordinate with "voluntary initiatives" related to identifying, categorizing, and reporting specified user-created content
13. Implement "age rating" and "age gating" systems covering all online content
14. Develop "parental control products" to limit the types of websites, social media platforms, and Internet content that can be accessed
15. Amend contracts with third parties, contractors, and affiliates to require their compliance with the Federal standards
16. Develop internal operational practices operational practices to "ensure" that third parties, contractors, and affiliates comply with the Federal standards

This is an elaborate list of both wide-ranging and granular requirements. Yet despite its breadth and granularity, the broad discretion to elaborate upon these themes—which is entirely given over to an ad hoc commission created by the bill—would authorize the promulgation of different or additional requirements that neither Congress nor the regulated community can predict. The specifics of such requirements as the mandatory takedown of user-created content are of enormous importance; yet they are nowhere defined in the bill, and the process for determining them would be wholly within the control of an unaccountable group of political appointees.

The several instances of requiring "searching for" specified user-created content, the requirement to store and preserve it, and the requirement to undertaking affirmative efforts to "prevent and disrupt" users' activity, together amount to a wide-ranging duty to monitor all incoming user-created content. It would otherwise not be possible to find what the websites are instructed look for; necessarily the entire haystack must be searched to find the needle. As protecting websites from having to monitor all user-created content is a fundamental purpose of Section 230, the EARN IT bill fails in this essential respect.

One would hope that, given the deeply intrusive nature of the EARN IT bill's proposed regulation of the businesses of millions of U.S.-based websites, as well as the extension of that regulation beyond websites and consumer-facing Internet platforms to a wide variety of Internet infrastructure providers, the Congress would be more solicitous of information concerning how its intended new standards would actually operate in the real world. While charging the commission to consider issues of cost and feasibility, there is no check on what the commission can actually prescribe.

Worse, there is no requirement for public input. Ordinarily, when Federal agencies promulgate rules, they are first subjected to public notice and opportunity to comment under the Administrative Procedure Act. When commissions are created to advise the executive branch, they are typically subjected to the requirements of the Federal Advisory Committee Act, which similarly ensures public transparency and input. But the EARN IT bill freezes out the public from any right of participation in the process of developing the new Federal standards. Instead, a commission comprised of politically-appointed individuals will have free rein to determine what Federal "best practices" are, without need of complying with either the APA or FACA. Among other things, this makes it far more likely that whatever standards are promulgated will be uninformed by considerations of how they will, or will not, function in practice.

Were I still a member of Congress, I would insist that, before this legislation proceeds further, it be amended to require the standard public notice and input that is expected for all Federal rulemakings.

Beyond the direct impact on websites from the significant compliance burdens that would attend compliance with these elaborate new Federal standards, the consequences for every American who uses the Internet would be more severe. Whereas today we take for granted the fact that our posts and communications via the Internet will be communicated instantaneously, compliance with the new requirements will mean that many user posts will have to be held in suspense, pending review by the website's legal team. Moreover, any user post that create risks to the platform is not likely to survive scrutiny, so that some messages will never be commu-

nicated at all. These unintended consequences will mark an unwelcome curtailing of the ease and speed with which Americans share their news and views online today.

Other aspects of the EARN It bill specifically touching upon Section 230 raise different issues.

The amended EARN IT Act carves out a wholesale exception to the law that extends to any claim made in a civil suit under any state law, provided it can be related to child sexual abuse material. The broad scope of the exception—it waives Section 230 state preemption completely—will make it an attractive exploitative opportunity for artful pleading. At a minimum, tightening up the language describing which claims are covered by the exception is required. The language in the PACT Act authorizing enforcement of Federal civil laws by state attorneys general is far preferable in this respect. It requires that the underlying claim must also allege a violation of Federal law.

An even more serious problem with this across-the-board waiver of Section 230 for all suits based on state laws is that the statutes of several states lack an actual knowledge standard. Instead, they predicate liability on recklessness. As a result, every website would be exposed to new lawsuits alleging that it was reckless in failing to actively monitor all user-created content. It is not difficult to imagine that such lawsuits could be successful. This would effectively impose a nationwide requirement of a duty to monitor—a result that Congress should wish to avoid, and that Section 230 was intended to prevent..

Since not only the new Federal standards but also the state-law litigation waived in by the EARN IT bill will strongly encourage monitoring and reporting, there will be new risks of constitutional challenges to criminal prosecutions using evidence reported in this way. Whereas under current law, companies are required only to report known instances of child sexual abuse material, EARN IT constitutes government inducement to actively search for it, and then turn it over for use by the government in prosecutions. This raises the prospect the what are now private searches would be deemed state action, subject to Fourth Amendment scrutiny.

With the exception of the 10th Circuit Court of Appeals (in an opinion written by then-Judge Neil Gorsuch),[30] most courts have held that the mandatory reporting arrangement under current law does not amount to state action, because the actual search that precedes the discovery of the evidence is done voluntarily.[31] But under applicable Supreme Court precedent, private searches are subject to the Fourth Amendment not only when the government requires a search, but when it merely encourages searches. And under the Exclusionary Rule, evidence collected in violation of the Fourth Amendment is generally inadmissible in court.

The risk posed by the EARN IT bill, therefore, is that evidence otherwise available to convict child abusers could now be suppressed.[32]

A further issue is that the amended EARN IT bill still threatens the privacy protections that websites can extend to their users. While the original version of the EARN IT bill posed a more direct threat to encryption, the amended version continues to give broad authority to its ad hoc commission to promulgate Federal standards that would give the government a "back door"—for example, by requiring websites to scan all data before and after encryption[33] or specifying that device manufacturers create custom operating systems allowing government access. (This is not idle speculation: the FBI attempted to convince Apple to do this four years ago.)

Finally, beyond these significant problems, the EARN IT bill's carveout for child sexual abuse material presents the same overall conceptual issue that was present during consideration of FOSTA/SESTA. The sexual exploitation of minors is a serious crime punishable under both Federal and state law. But it is one of approximately 4,000 Federal crimes and thousands more state law crimes that include terrorism, extortion, mass murder, airline hijacking, rape, hate crimes, hostage taking, sexual battery, torture, and treason. Any one of these crimes can be facilitated using the internet. As with the telephone and the telegraph before it, the Internet is frequently a tool of criminals. Section 230, which is designed to apply a uniform Federal standard in all civil and criminal cases brought in either state or Federal fo-

---

[30] *United States v. Ackerman,* 831 F.3d 1292, 1302 (10th Cir. 2016). *see also, e.g., United States v. Coyne,* 387 F.Supp.3d.

[31] *See, e.g. United States v. Coyne,* 387 F.Supp.3d.387 (2018).

[32] *See* Chris Marchese, *The EARN IT Act's Collision Course With The Fourth Amendment* (2020), *https://netchoice.org/wp-content/uploads/2020/06/EARN-It-4A-Report-FINAL.pdf.*

[33] As one observer has noted, the popular euphemism for this—"client-side scanning"—is what we would otherwise call "reading your messages on your device." Carl Szabo, "The EARN IT Act threatens encryption," *Orange County Register* (July 14, 2020).

rums, is wholly consistent with the prosecution of criminal and civil claims based on the entire range of illegal activity of which humankind is capable.

It is difficult to argue that, as horrible as the promotion of child pornography is, it is categorically worse than mass murder, terrorism, and a long list of other equally egregious crimes. Nor are these other crimes any less worthy of congressional attention. As Chairman of the House Committee on Homeland Security, I saw firsthand how terrorists use the Internet to direct violent extremist acts. Neither in America nor anywhere in the world should terrorists find a "safe space" to operate and disseminate their murderous propaganda of mass destruction. When violent extremists further their plots and grow their ranks by use of the internet, it stands to reason that a nation of laws would not wish to permit laws enacted for another purpose to be used as a shield for such acts. Likewise, when criminal gangs kidnap innocent tourists for exorbitant ransom, using threats of torture and murder, no law should provide them any form of immunity. When assassins target our president, lawmakers, or Supreme Court, no one would want to grant the murderers a legal advantage because they happened to use the Internet in the commission of their crimes.

Yet the EARN IT bill would treat these problems categorically differently for legal purposes, providing one set of rules for child sexual abuse material and another, presumably more lenient, set of rules for terrorism.

This represents a fundamental misunderstanding of how Section 230 is intended to operate. It was designed to protect the innocent from being held liable for wrongs committed entirely by others—a principle that should not be waived in any circumstances. It was equally intended to ensure that those who actually commit wrongs will be subject to prosecution by both civil and criminal law enforcement. One need not rely on the legislative history or the words of the authors for this proposition. The language of the statute is plain enough. If a website, or anyone who provides what the law describes as interactive computer services, is complicit in the creation of unlawful content then it may not claim protection under Section 230.

Section 230, as written and as interpreted by the courts, is thoroughly consistent with the aggressive prosecution of child sexual exploitation. Equally importantly, it is thoroughly consistent with the aggressive prosecution of all other crimes. It makes little sense to countenance an interpretation of Section 230 that communicates to judges looking at prior decisional law that henceforth, a less stringent rule will be applied in all but the narrow categories carved out of Section 230 by Congress. Each carveout for differential treatment will create significant new legal ambiguities and inexplicable horizontal disparities in both Federal and civil litigation. Judges faced with a new Section 230 standard for sex trafficking and child sex abuse cases will be hard pressed not to infer that cases involving other crimes must be decided using a different rule.

It is notable that the most of the Nation's attorneys general have written to Congress endorsing a different approach—one that will encompass not only child sexual abuse but all criminal enforcement actions. Such an approach would ensure that courts do not decide to make some Internet crimes easier, and some crimes harder, to prosecute. While it would be a mistake to do this by scrapping the uniform Federal policy with respect to liability for Internet platforms, it is unquestionably correct that uniformity in the application of the Federal policy to all crimes is necessary to prevent unintended consequences such as the creation of loopholes that benefit criminals.

Conclusion

I applaud the efforts of Senators on this subcommittee and on the full committee to undertake a thoughtful and dispassionate analysis of the several competing interests involved in keeping the Internet free from illegal content and conduct, while at the same time promoting and protecting a vibrant Internet ecosystem with the maximum level of free expression. As the co-author of Section 230, which has proven to be a foundational legal underpinning for the Internet as it has developed over the last quarter century, I am proud of the role that this law has played in empowering the millions of content creators on the internet, and for the protections it has effectively provided for the freedom of speech of millions of people.

Our reconsideration of the scope of Section 230's protections comes at a time in world history when digital authoritarianism is spreading rapidly around the globe. As Freedom House has noted in its most recent annual report on the state of global Internet freedom entitled *Freedom on the Net,* "repressive regimes, elected incumbents with authoritarian ambitions, and unscrupulous partisan operatives have exploited the unregulated spaces of social media platforms, converting them into in-

struments for political distortion and societal control."[34] They note that while social media in other nations have at times served as a level playing field for civic discussion, they now more often expose citizens to unprecedented invasions of their fundamental freedoms, as governments deploy advanced tools to identify and monitor users on a vast scale. This abuse of social media is occurring not just in well-known cases such as the People's Republic of China, Russia, Iran, and Saudi Arabia, but also in 38 of the 65 countries covered in their latest report.

America's approach to the regulation of social media, and of speech on the Internet more generally, has to date followed a very different model, abjuring government control in favor of private ordering. This has led some critics to argue that private control of the vast amounts of information generated by users of the Internet represents a threat to liberty and privacy equal to or greater than would be the result of government control. But two factors militate against this conclusion. Importantly, the private websites and platforms with access to user data are many, and compete with one another. And they lack the powers of a sovereign to aggregate all available data and then to regulate the citizenry through its exploitation. In the hands of government, social media surveillance tools employing artificial intelligence can easily become powerful weapons with which to silence undesirable expression and exert social control.

Before taking even the first baby steps away from the policy Congress and the president endorsed in Section 230 "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation," legislators should be fully aware of where this road could lead.

The landscape of the Internet continues to change rapidly, and therefore demands continued vigilant oversight and critical scrutiny by lawmakers. Section 230 is the creation of Congress, and subject to its plenary authority to make and revise laws. It is not written in stone and far from sacrosanct. But it has also provided us with the benefit of a quarter century of practical experience, through continually changing and often challenging circumstances. In the main, it has performed well. To the extent that courts applying it have sometimes given us unwanted results, we can take comfort in the fact that as of 2020 the interpretive kinks that in the past have sometimes let wrongs go without remedy have been for the most part worked out.

Were I still in Congress, though I would be tempted to embellish my original work (like the artist who continues to add a daub here and a brushstroke there, with the result that the painting is never finished), in the current environment I would hesitate to do so. My far greater concern would be the risk, which I have so often seen materialize in the completion of legislation with which I have been involved, that the process of moving the bill through numerous committees, markups, and perhaps an ultimate conference between House and Senate would ultimately run away with my best intentions.

Unlike the placid policymaking environment in which Section 230 was conceived and midwifed into law in 1995–96, today the cacophony that is the debate over social media, content moderation, free speech, and criminality on the Internet guarantees not only near-irreconcilable conflicts but also legislative attempts to somehow square the circle. Such deep compromises ranging from the smallest details to high-level issues, which will be necessary if a Republican Senate and Democratic House are to reach any agreement on a bill that achieves their very disparate aims, will likely produce legislation far different from the careful balancing of competing interests that this committee's thoughtful and dispassionate analysis is admittedly capable of producing in the first instance.

In my judgment, the chance that in the end the most important benefits of Section 230 could be undermined, or lost entirely, is a gamble with the future of the Internet not worth taking. Recognizing that it is your own judgments on these questions that matter, and that those judgments await your completion of your ongoing analysis of the many issues involved, I stand ready to assist you in any way that I can.

Senator THUNE. Thank you, Mr. Cox.
Next up is Mr. Jeff Kosseff.
Mr. Kosseff, please proceed.

---

[34] *Freedom on the Net 2019: The Crisis of Social Media,* available at *https://freedomhouse.org/report/freedom-net/2019/crisis-social-media*

STATEMENT OF JEFF KOSSEFF, ASSISTANT PROFESSOR, CYBER SCIENCE DEPARTMENT, UNITED STATES NAVAL ACADEMY

Mr. KOSSEFF. Chairman Thune, Ranking Member Schatz, and members of the Subcommittee, thank you for providing me with the opportunity to testify about the history and purpose of Section 230.

I'm an assistant professor in the Cyber Science Department in the U.S. Naval Academy. My testimony today reflects only my personal views and does not represent the Naval Academy, Department of Navy, Department of Defense, or any other party.

This hearing is of the utmost importance, as Section 230 is responsible, more than any other law, for the open Internet that Americans know, love, and hate. I am not here today to advocate for or against any particular legislation. Rather, my goal is to help expand the public understanding of Section 230.

As explained in detail in my written testimony, under the First Amendment and common law, distributors cannot be held liable for content created by others unless the distributors knew, or had reason to know, of the illegal content. A New York trial judge in 1995 ruled that Prodigy did not receive this distributor protection and, instead, was deemed a publisher that's liable, regardless of its state of mind. The judge's reasoning was that Prodigy has implemented detail user conduct rules and employed content moderating.

Members of Congress passed Section 230 in 1996 in an effort to override this decision and encourage platforms to moderate. Some critics argue that platforms have not adequately moderated harmful content. Other critics argue that some existing moderation practices result in blocking certain political viewpoints. And both criticisms have driven a number of proposals to change Section 230.

Today, I hope to set forth some principles to guide your evaluations of Section 230s future:

First, not all problems on the Internet are Section 230 problems. For instance, the First Amendment, and not Section 230, protects hate speech. Additionally, many defamation claims that courts dismiss on Section 230 grounds would also, if fully litigated, not survive common law and First Amendment protections.

Second, we do not know with certainty how platforms would react to a repeal or a significant contraction of Section 230, because the modern Internet has always existed with Section 230 in place. One possibility is, the platforms might avoid moderation, fearing that, once they encounter potentially actionable content, they would become liable for it. There's also the chance that there would be fewer venues for user-generated content.

Third, Section 230 is designed to encourage, and not discourage, moderation of user content. In the debate over neutrality of platforms, I see a few different questions:

First, does Section 230 currently require neutrality? As I explained in my written testimony, the answer to this question is no.

Second, should Section 230 require neutrality? The answer to this question is up to you, as Congress is free to amend Section 230 as it sees fit; of course, within the confines of the First Amendment.

If Section 230 were to attempt to impose a neutrality requirement, I would ask what such a requirement would look like, and how it would be implemented. Of course, Congress can, and should, determine whether the market-based system under Section 230 continues to meet users' expectations in 2020.

Fourth, the Section 230 debate needs far more transparency. Last October, I suggested the creation of a congressionally chartered commission to gather facts and recommend a path forward. The Cyberspace Solarium Commission provides an excellent model for this.

I commend the Chairman and Ranking Member for the thoughtful solutions that you've proposed in the PACT Act. The legislation addresses the need for more transparency and content moderation policies, and begins the process of identifying the most tailored and reasonable rules for providing that transparency. The bill also provides people with a mechanism to take down material that has been adjudicated to be defamatory or illegal under Federal criminal or civil law. We must ensure that a takedown provision is not abused, for example, via the falsification of court orders.

As I routinely remind technology companies, Section 230 is not set in stone and can be repealed or significantly amended as easily as it was passed. Congress may determine that it is in the public interest to curtail some or all of Section 230s protections. I urge you to make any such decisions with great care.

It is difficult to imagine how some of the largest companies in the United States could have emerged, at least in their current forms, without Section 230. The challenge for all of us is to determine how we want the Internet to look over the next 25 years, and what it takes to get it.

I look forward to taking your questions.

[The prepared statement of Mr. Kosseff follows:]

PREPARED STATEMENT OF JEFF KOSSEFF, ASSISTANT PROFESSOR, CYBER SCIENCE DEPARTMENT, UNITED STATES NAVAL ACADEMY

Chairman Thune, Ranking Member Schatz, and Members of the Subcommittee, thank you for providing me with the opportunity to testify about the history and purpose of Section 230 of the Communications Decency Act of 1996.

I am an assistant professor in the Cyber Science Department of the United States Naval Academy. My testimony today reflects only my personal views, and does not represent the Naval Academy, Department of Navy, Department of Defense, or any other party.

It is difficult to overstate the importance of the subject of this hearing. Last year, I published a history of Section 230, titled *The Twenty-Six Words That Created the Internet.* The Internet's protocols and technology were developed long before 1996. But Section 230 is responsible, more than any other law, for the open Internet that Americans know, love, and hate. By shielding online platforms from liability for a great deal of third-party content, Section 230 has paved the way for Yelp, Wikipedia, Facebook, Twitter, YouTube, and so many other online services. These have primarily based their business models on content created by individuals rather than corporations. Section 230 also has protected a wide range of companies of all sizes that operate websites with user comments.

When I began writing a book about Section 230 in 2016, few people outside of technology law and policy circles knew much about what the law does and why Congress passed it in 1996. Much has changed in those four years, as large platforms are under unprecedented scrutiny for their handling of user-generated content. Suddenly, Section 230 has moved from obscure legal discussions to the headlines of major media organizations. Many are calling for you to repeal or amend Section 230. Indeed, there are many legislative proposals, including a thoughtful one from the Chairman and Ranking Member of this subcommittee.

I am not here today to advocate for or against any particular legislation. Rather, my goal is to help expand the public understanding of Section 230, first by providing an overview of its history and purpose, and then by suggesting principles that could guide Congress as it considers Section 230s future.

I. The History of Section 230

To understand why we have Section 230 and what it does, we need to look at how platform liability worked before it was passed. This requires an examination of the liability standards for bookstores and other distributors of content produced by third parties.

The foundations for distributor liability standards come from *Smith v. California,*[1] a 1959 Supreme Court opinion. In that case, the Court reversed the conviction of a Los Angeles bookstore owner whose store sold an obscene book. The ordinance under which he was convicted imposed criminal liability on bookstore operators regardless of their scienter or state of mind; in other words, the ordinance was one of strict liability on any distributor of obscene content, regardless of their intention or even awareness. Writing for the majority, Justice Brennan recognized that obscenity is not protected by the First Amendment, but he concluded that imposing strict liability on booksellers nonetheless *did* violate the First Amendment because such a rule would chill non-obscene speech.

"By dispensing with any requirement of knowledge of the contents of the book on the part of the seller, the ordinance tends to impose a severe limitation on the public's access to constitutionally protected matter," Justice Brennan wrote. "For if the bookseller is criminally liable without knowledge of the contents, and the ordinance fulfills its purpose, he will tend to restrict the books he sells to those he has inspected; and thus the State will have imposed a restriction upon the distribution of constitutionally protected as well as obscene literature."[2]

The Court in *Smith* refrained from articulating the precise mental state necessary to impose liability on distributors of third-party content, only saying that strict liability is unacceptable.[3] The Supreme Court would provide a bit more guidance. For instance, in 1968, the Court upheld a New York law that imposed criminal liability on a newsstand that sold pornographic magazines to minors.[4] The statute applied to stores that have "general knowledge of, or reason to know, or a belief or ground for belief which warrants further inspection or inquiry" of both the character and content of material that is "reasonably susceptible of examination by the defendant" as well as the minor's age.[5] Writing for the majority, Brennan concluded that this level of awareness satisfies the concerns that he articulated in *Smith,* though he again refrained from setting a precise minimum standard for all distributor cases.[6]

Following *Smith v. California*—but prior to the passage of Section 230—lower courts generally adopted a rule, rooted in the common law and the First Amendment, that distributors cannot be liable for content created by others unless the distributors knew or had reason to know of the illegal content. This rule applies not only to criminal obscenity cases, but also to civil claims such as defamation.[7]

This common law rule was first applied to an online service in 1991, in a defamation action against CompuServe, one of the earliest national online dial-up services. The suit arose from statements in an online newsletter that CompuServe distributed. The district court dismissed the lawsuit, concluding that CompuServe was "in essence an electronic, for-profit library that carries a vast number of publications and collects usage and membership fees from its subscribers in return for access to the publications."[8] In other words, CompuServe was a distributor, and therefore deserved the same liability standards to which newsstands were held.[9] Because the plaintiff had not demonstrated that it knew or had reason to know of the alleged libel in the newsletter, the court dismissed the case.

---

[1] Smith v. California, 361 U.S. 147 (1959).
[2] *Id.* at 153.
[3] *Id.* at 154–55.
[4] Ginsberg v. New York, 390 U.S. 629 (1968).
[5] *Id.* at 646.
[6] *Id.* at 644–45.
[7] *See, e.g.,* Dworkin v. Hustler Magazine, 611 F. Supp. 781 (D. Wyo. 1985); Osmond v. Ewap, 153 Cal. App. 3d 842 (Cal. Ct. App. 1984).
[8] Cubby v. CompuServe, 776 F. Supp. 135, 140 (S.D.N.Y. 1991).
[9] *Id.* Crucially, the court acknowledged that even a distributor such as CompuServe could have some control over the content that it distributed. *See id.* ("While CompuServe may decline to carry a given publication altogether, in reality, once it does decide to carry a publication, it will have little or no editorial control over that publication's contents. This is especially so when CompuServe carries the publication as part of a forum that is managed by a company unrelated to CompuServe.").

CompuServe's main competitor at the time was Prodigy, which sought to distinguish itself from CompuServe by offering more family-friendly services. Prodigy employed contract moderators and implemented detailed user conduct rules. When Prodigy was sued due to comments made on a Prodigy financial bulletin board, the company attempted to claim the same distributor liability standard to which CompuServe was held. In May 1995, a New York state trial court judge rejected Prodigy's attempt, finding that Prodigy is not a distributor, but rather a publisher that is liable regardless of whether it knew or had reason to know of the allegedly defamatory content. Even though, by 1995, Prodigy had loosened its user content policies, the Court focused on the fact that Prodigy had at one point exercised substantial control over user content. "It is Prodigy's own policies, technology and staffing decisions which have altered the scenario and mandated the finding that it is a publisher," the judge wrote. "Prodigy's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice."[10]

The *Stratton Oakmont v. Prodigy* case received significant media attention. Although it did not create binding precedent, it strongly suggested that online services could reduce their exposure to liability by taking a hands-off approach to user content. If, like Prodigy, a platform exercised significant control over user content, a court might conclude that it does not receive the same "distributor" liability standards as a bookstore or newsstand. I believe the ruling was flawed because it ignored the fact that even the more hands-off CompuServe could choose not to carry a publication in its electronic version of a newsstand. And even if a platform received the liability standard of a "distributor," it still could face liability if it knew of, or had reason to know of, illegal content, creating another disincentive to moderation.

When Reps. Chris Cox and Ron Wyden learned about the *Prodigy* case, they agreed that it made little sense. Why subject an online service to more liability simply because it took steps to moderate objectionable content? This disincentive was particularly concerning as schools and homes increasingly connected computers to the Internet. If the legal system discouraged online services from moderation, the result could be the exposure of children to pornography and other objectionable material. A bill in the Senate, the Communications Decency Act of 1995, sought to address this problem by imposing criminal liability for the transmission of indecent content. The Senate attached this decency proposal to its massive overhaul of U.S. telecommunications law.

Cox and Wyden believed that the online services—which are accountable to their users—are better positioned than the government to set user content policies. They saw the potential for the Internet to be an engine for job growth. They did not want to stifle this burgeoning new technology with regulation and litigation. Nor did they want to impose a duty of pre-screening user content before it was posted.

On June 30, 1995, Cox and Wyden introduced the Internet Freedom and Family Empowerment Act, most of which would later become Section 230. To address the prospect of government regulation, the bill initially stated that the Federal Communications Commission does not have authority "with respect to economic or content regulation of the Internet or other interactive computer services."[11]

The centerpiece of the bill, however, focused on the liability of online platforms for user content, and the need to eliminate any disincentive to moderation. The provision that contains what I believe are the 26 words that created the Internet states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[12] The bill also prevents interactive computer service providers and users from being liable for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected"[13] or providing the technical means to restrict access.[14]

Cox and Wyden included exceptions for the enforcement of Federal criminal law,[15] intellectual property law,[16] and Federal and state electronic communications privacy

---

[10] Stratton Oakmont v. Prodigy Service Co., 23 Media L. Rep. 1794 (N.Y. Sup. Ct. May 24, 1995).

[11] This provision would not remain in Section 230 as signed into law.

[12] 47 U.S.C. § 230(c)(1). As initially introduced, this provision actually contained 25 words because it stated: "No provider or user of interactive computer services shall be treated as the publisher or speaker of any information provided by an information content provider."

[13] 47 U.S.C. § 230(c)(2)(A).

[14] 47 U.S.C. § 230(c)(2)(B).

[15] 47 U.S.C. § 230(e)(1).

[16] 47 U.S.C. § 230(e)(2).

laws.[17] The bill was partly based on a theory of user empowerment: the belief that users, with tools provided by their platforms, should determine what content should be available to them and their children.

To clarify their intentions, Cox and Wyden included findings at the start of their bill. Among their findings: "These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops."[18] Cox and Wyden also wrote that the "Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[19] The Internet has "flourished, to the benefit of all Americans" they wrote, "with a minimum of government regulation."[20]

They also included statements of policy, including "to promote the continued development of the Internet and other interactive computer services and other interactive media"[21] and "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services."[22] They also wrote that it is U.S. policy "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[23]

On Aug. 4, 1995, the House debated whether to add the Cox-Wyden proposal to its version of what would become the 1996 telecommunications overhaul. The House members almost uniformly welcomed the proposal as an alternative to the Senate's indecency proposal, which many viewed as unconstitutional. "Really it is like saying that the mailman is going to be liable when he delivers a plain brown envelope for what is inside it," Rep. Zoe Lofgren said of the Senate proposal. "It will not work."[24]

Rep. Robert Goodlatte spoke of the need to fix the perverse incentive created by the Prodigy opinion. "The Cox-Wyden amendment removes the liability of providers such as Prodigy who currently make a good faith effort to edit the smut from their systems," Goodlatte said. "It also encourages the online services industry to develop new technology, such as blocking software, to empower parents to monitor and control the information their kids can access."[25]

Cox spoke about the need to avoid Federal regulation of the Internet. The bill, he said, "will establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet, that we do not wish to have a Federal Computer Commission with an army of bureaucrats regulating the Internet because frankly the Internet has grown up to be what it is without that kind of help from the Government."[26]

The House voted 420–4 to attach Cox and Wyden's amendment to its version of the Telecommunications Act. As a compromise, the conference committee included both the Senate's Communications Decency Act and the House's amendment in the same Title of the telecommunications law. Hence, the Cox-Wyden provision became known as "Section 230 of the Communications Decency Act," even though it had not been introduced under with that title. Section 230 appeared largely as Cox and Wyden proposed it, though it no longer contained the provision that banned FCC regulation of Internet content. The final version also added an explicit statement that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[27]

From the relatively sparse legislative history, it is clear that Section 230s drafters had two primary goals. First, they wanted to ensure that the nascent commercial Internet was unburdened from regulation and litigation. Second, they wanted to encourage online providers to moderate as they (and their users) saw fit. In the short discussion of Section 230 in the conference report for the Telecommunications Act, the conferees wrote that they intended to overrule the *Stratton Oakmont v. Prodigy* decision, and that "such decisions create serious obstacles to the important Federal

---

[17] 47 U.S.C. § 230(e)(4).
[18] 47 U.S.C. § 230(a)(2).
[19] 47 U.S.C. § 230(a)(3).
[20] 47 U.S.C. § 230(a)(4).
[21] 47 U.S.C. § 230(b)(1).
[22] 47 U.S.C. § 230(b)(3).
[23] 47 U.S.C. § 230(b)(2).
[24] 141 Cong. Rec. H8471 (1995).
[25] 141 Cong. Rec. H8471–72 (1995).
[26] 141 Cong. Rec. H8470 (1995).
[27] 47 U.S.C. § 230(e)(3).

policy of empowering parents to determine the content of communications their children receive through interactive computer services."[28]

On the day that President Clinton signed the Telecommunications Act into law, civil liberties groups challenged the Senate's indecency provisions, and the next year the Supreme Court would strike them down as unconstitutional.[29] The Supreme Court's ruling did not affect Section 230. In fact, the civil liberties groups that challenged the Communications Decency Act took care to not include Section 230 in their litigation, recognizing the need to preserve Section 230.

Section 230 received little attention in the months after it was passed. This was in part because it was unclear how broadly courts would interpret the 26 words. It was possible to read Section 230 as merely conferring distributor liability standards to all interactive computer service providers; in other words, a platform still could be liable if it knew or had reason to know of the illegal user content. A second, broader reading, would bar the platform from having any liability for content provided entirely by third parties, unless an exception applied.

This uncertainty ended on Nov. 12, 1997, when the United States Court of Appeals for the Fourth Circuit adopted the latter, broad reading of Section 230 in *Zeran v. America Online.* Distributor liability, Judge J. Harvie Wilkinson wrote, "is merely a subset, or a species, of publisher liability.[30] Thus, Wilkinson concluded, when Section 230 states that an interactive computer service provider shall not be "treated as the publisher or speaker" of information provided by a third party, the statute also bars distributor liability. "Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum," Judge Wilkinson wrote.[31]

Wilkinson recognized that subjecting an online service such as America Online to notice-based liability likely would cause these services to remove user content upon notice, even if the content was not defamatory. "Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information," he wrote. "Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context."[32]

Because Judge Wilkinson was the first Federal appellate judge to interpret Section 230, judges nationwide adopted his ruling in *Zeran v. America Online,* and the broad reading of Section 230 became the law of the land. Cox and Wyden—the authors of Section 230—told me as I was researching my book that they agreed with Wilkinson's interpretation. But it is possible to see how another judge might have concluded that Section 230s scope if more limited.

The *Zeran* reading of Section 230 eliminates the *Stratton Oakmont v. Prodigy* problem by preventing platforms from becoming liable for user content they are unaware of simply because they have moderated some other content. But it goes much further than that; it also allows platforms to decide whether to keep up or take down content that they *are* aware of without facing potential liability for that content. And that is how Section 230 has created the legal framework for the Internet that we know today.

Imagine how a social media site might behave had Judge Wilkinson determined that Section 230 only means that all platforms be held to a distributor liability standard. The site could face liability if it knew or had reason to know of defamatory or otherwise actionable user content. Such a liability regime might discourage the social media site from actively moderating user content, as it might face liability for content that it learned about but failed to remove. A social media site with millions or billions of users is in no position to investigate every user post and determine whether it is defamatory or otherwise illegal. Section 230, as Judge Wilkinson interpreted it, removes that disincentive to moderation.

Thanks to Judge Wilkinson's interpretation, Section 230 has protected a wide range of platforms from many different types of claims. As I detail in *The Twenty-Six Words That Created the Internet,* this sweeping protection has been vital for con-

---

[28] H. Rep. 104–458 at 194.
[29] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).
[30] Zeran v. America Online, 129 F.3d 327, 332 (4th Cir. 1997).
[31] *Id.* at 330.
[32] *Id.* at 333.

sumer review sites,[33] Wikipedia,[34] social media,[35] search engines,[36] and countless other sites that have built their business models around user-generated content.

Yet Section 230 also has shielded platforms in some cases in which the plaintiffs have suffered serious harms. Among the lawsuits in which courts held that Section 230 applies is one that involved a dating app that was used to impersonate a man. The advertisements, posted by his ex-boyfriend, claimed that the man wanted to engage in rape fantasies or role play. This caused about 1,100 men to respond to the ads, receiving the man's home and workplace locations via the app's geolocation function. Many men visited his home and work, demanding sex and drugs. The man said he contacted the app about 100 times, and only received an automated response.[37] He sued the app under a number of theories of liability, including negligence, infliction of emotional distress, products liability, and negligent design, but the district court dismissed the claims on Section 230 grounds, and the Second Circuit affirmed the dismissal.[38] The district court also refused to extend an earlier state court temporary restraining order that required the app to "immediately disable" profiles that impersonated the plaintiff. Section 230 has protected a gossip website that encourages users to submit "the dirt" and selects which submissions to post and highlight.[39] And it has protected social media platforms used by terrorists, even when the platform's algorithms helped make that user content visible.[40] As long as the website operator has not taken part in the creation of the user content and an exception does not apply, Section 230 will protect the website from liability arising from the display and moderation of content created by others. Section 230 does not block a plaintiff from suing the person who created the harmful content, but there are a number of reasons why that might not be practical, including the inability to track down the poster and fear of retaliation.

In short, Section 230 has fostered an Internet in the United States that faces less regulatory and litigation burden than in other countries, including other western democracies. This open Internet has created many social benefits, but others have suffered real and serious harms. For a broad perspective about the benefits and costs of the Internet as governed by Section 230, I encourage you to read *Hate Crimes in Cyberspace* by Danielle Citron, *The Cult of the Constitution* by Mary Anne Franks, *The Splinters of Our Discontent* by Mike Godwin, and *Nobody's Victim* by Carrie Goldberg.

II. Principles for Evaluating the Future of Section 230

Over the past year, Section 230 has been in the news more than any other time in its nearly 25-year history. Often, the news is not positive. Some critics argue that platforms have not adequately moderated harmful content and have failed to achieve Congress's goal of establishing content moderation systems that meet the needs of their users. Other critics argue that some existing moderation policies and procedures result in blocking certain political viewpoints.

Both criticisms have driven a number of proposals to change Section 230. I am not here today to endorse or propose any particular change to Section 230. Rather, I hope to set forth some principles to guide your evaluation of Section 230s future. I derive these principles from my research into Section 230s history, and the impacts of courts' interpretation of Section 230 over nearly a quarter century.

A. Not All Problems on the Internet Are Section 230 Problems

I recognize that this principle may sound odd coming from a professor who asserts that Section 230 created the Internet. I maintain that Section 230 provided the legal framework that allowed platforms to structure their business models around user-generated content. But that does not mean that every flaw in the current system is attributable to Section 230. There is a lot to love about the Internet, but there also is a lot not to love about the Internet. Some content is vile. Some ruins lives. Some does lasting damage to society and our institutions. But before placing all of the blame for this content on Section 230, it is important to first examine whether a cause of action exists for that harm. If a cause of action does not exist, then there is nothing for Section 230 to block.

For instance, a big headline on the cover of the *New York Times* business section last August proclaimed: "Why Hate Speech on the Internet is a Never-Ending Prob-

---

[33] Kimzey v. Yelp! Inc., 836 F. 3d 1263 (9th Cir. 2016)
[34] Bauer v. Glatzer, Docket No. L–1169–07 (Superior Court of N.J., Monmouth County, 2008)
[35] Doe v. MySpace, 528 F.3d 413 (5th Cir. 2008).
[36] Fakhrian v. Google, No. B260705 (Cal. Ct. App. April 25, 2016)
[37] Herrick v. Grindr, 306 F. Supp. 3d 579, 585 (S.D.N.Y. 2018).
[38] Herrick v. Grindr, No. 18–396 (2d Cir. Mar. 27, 2019) (not precedential).
[39] Jones v. Dirty World Entertainment Recordings, 755 F.3d 398 (6th Cir. 2014).
[40] Force v. Facebook, 934 F.3d 53 (2d Cir. 2019).

lem." Below the headline were the key 26 words from Section 230, followed by: "Because this law shields it." The Times later appended the following dramatic correction to the story: "An earlier version of this article incorrectly described the law that protects hate speech on the internet. The First Amendment, not Section 230 of the Communications Decency Act, protects it." Despite the correction, later that month, a Federal judge cited this article while describing the debate over "Section 230s grant of immunity for speech-based harms such as hate speech or libel."[41] To be sure, online hate speech is a serious problem, but the reality is that the First Amendment protects hate speech, regardless of Section 230. Of course, the Supreme Court's First Amendment jurisprudence could evolve to treat hate speech differently—and some believe it should. And even now, if that hate speech also is illegal for some other reason (for example, because it is a true threat or defamatory), then it could fall outside the scope of First Amendment protection. But hate speech, standing alone, is constitutionally protected. Changing Section 230 would not change platforms' legal obligations in this area.

Many defamation claims that courts dismiss on Section 230 grounds would also, if fully litigated, not survive common law and First Amendment protections. These include the requirement for falsity, the opinion privilege, and the actual malice bar for public officials and figures. Because Section 230 provides strong procedural protections, defamation lawsuits against platforms often are decided in the early stages, eliminating the need for the parties to engage in extensive discovery and for courts to decide fact-intensive questions about defamation law. Additionally, as seen in the 1950s bookseller cases, the First Amendment and common law provide some protection to distributors of content created by others. As I describe in the next subsection, there is uncertainty as to how extensive that protection is.

In addition to hate speech concerns, large companies—including big technology platforms—have been rightly criticized for their privacy and data security practices. These are serious problems that I hope Congress will address with comprehensive and effective laws that set tough national standards for privacy and cybersecurity. Section 230, however, is not at the root of these problems. Section 230 only protects platforms from liability for third-party content; it does not affect their liability after a data breach or generally shield their data collection practices.

Nor does Section 230 have any link to copyright infringement. From the beginning, Section 230 has had an exception for intellectual property law. Platforms and content creators have long been engaged in a spirited debate over the notice-and-takedown system established by an entirely different law, the Digital Millennium Copyright Act. Unfortunately, recent media reports have conflated Section 230 and the DMCA. Likewise, Section 230 always has had an exception for the enforcement of Federal criminal law, so user content that constitutes a Federal crime is not covered by the statute's protections.

B. We Don't Know How Platforms Would React to a Repeal or Significant Contraction of Section 230

Although there are not any legislative proposals to repeal Section 230, repeal has been publicly suggested in the media, and it is important to examine what the Internet might look like without Section 230. Moreover, eliminating Section 230 protections for a particular type of content might have a similar impact on some platforms.

Because Section 230 has been on the books since 1996, it is difficult to know with certainty what the Internet would look like without it. This uncertainty stems from the lack of caselaw that extrapolates common law liability standards to modern online platforms. We can only look at cases involving bookstores, and the few nonbinding opinions involving Prodigy and CompuServe that were decided before Section 230s passage.

If courts were to adopt the *Stratton Oakmont v. Prodigy* line of thinking, platforms would fear being dubbed "publishers," who are subject to the same liability for user content as the authors, rather than "distributors," who are liable only if they knew or had reason to know of the illegal content. I believe that the judge in this case got the law wrong, drawing an artificial line between a publisher that exercises "editorial control" and distributor, when all distributors exercise some degree of editorial control (for instance, a bookstore could refuse to sell a certain book). Still, there is no guarantee that courts would disagree with the *Stratton Oakmont* decision. If it were widely adopted, this reasoning likely would discourage platforms from engaging in any moderation, lest they be dubbed common-law "publishers."

If courts were to reject the *Stratton Oakmont v. Prodigy* holding (as I hope they would), online platforms could face liability if they knew or had reason to know of

[41] Papataros v. Amazon.com, Civ. No. 17–9836 (D. N.J. Aug. 26, 2019).

the illegal content. This might result in a system in which anyone could complain to a platform about user content, regardless of the merit of their complaints, at which point a platform that did not take down the content would risk being forced to defend it in court. Platforms also might avoid moderation, fearing that once they encounter potentially defamatory or otherwise actionable content, they would become liable for it. Complicating matters, it is unclear when a platform would have a "reason to know" of illegal content, as there is very little caselaw that articulates when a distributor has "reason to know." For instance, this might expose a platform to liability if it generally knew that users posted defamatory material, but had not seen the particular post in question.

In the landmark *Zeran* case, Judge Wilkinson warned that it was "impossible" to expect platforms to screen user content. "Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted," he wrote. "Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect."[42] Indeed, it is conceivable that some platforms might reduce or entirely eliminate user content in a world without Section 230s protections.

A change to Section 230—even short of full repeal—may have significant impacts on platforms' operations. For instance, when Congress amended Section 230 in 2018 to create an exception for certain civil actions and state criminal cases involving sex trafficking, Craigslist removed the personals section it had hosted for years. "Any tool or service can be misused," Craigslist wrote. "We can't take such risk without jeopardizing all our other services, so we have regretfully taken craigslist personals offline."

C. Section 230 is Designed to Encourage—Not Discourage—Moderation of User Content

In my decade writing about Section 230 and practicing Internet law, I have encountered far too many lawyers who advise website operators that if they moderate user content, they will lose their Section 230 protections. I fear that this has caused websites to take a hands-off approach to user content that they otherwise would have blocked.

This advice is simply incorrect. Section 230s protections do not disappear merely because a platform has engaged in content moderation. As Section 230s legislative history makes clear, one of the main purposes of Section 230 was to encourage online service providers to moderate. Indeed, the title of the most important section of the statute is "Protection for 'Good Samaritan' Blocking and Screening of Offensive Material."

To be sure, Section 230 does not *require* moderation. Rather, the law leaves it up to the providers to determine what moderation—and moderation tools—to provide to their users. Section 230 is very much a market-based law, based on the assumption that user demands will dictate platforms' moderation approaches.

Of course, Congress can and should determine whether the market-based system continues to meet users' expectations in 2020, when a handful of platforms have market capitalizations that are greater than those of automakers. We are in a very different world than 1996, when 40 million people worldwide had Internet access, and being suspended from Prodigy was unlikely to have significant consequences to one's livelihood. Suspension from a large social media platform in 2020, on the other hand, has a much greater impact.

In the debate over "neutrality" of platforms, I see a few different questions. First: Does Section 230 currently require neutrality? Second: Should Section 230 require neutrality?

The answer to the first question, as explained above, is "no." The answer to the second question is up to you, as Congress is free to amend Section 230 as it sees fit. If Congress were to attempt to impose a neutrality requirement, I would ask what such a requirement would look like, and how it would be implemented. Moderation often requires difficult judgments about content being transmitted at a furious pace. Could a platform block *any* content while still remaining "neutral?" Would a "neutral" Internet full of legal pornography, threats, bullying, or encouragement of anorexia be an improvement? Even if this neutrality requirement were limited to political speech, some political debates can border on hate speech. If a platform were to moderate a political discussion for violating its hate speech policies, would that violate a neutrality requirement? These questions are tough to answer in the abstract, and even more difficult when presented with the torrent of choices that platforms must make every minute.

---

[42] Zeran v. America Online, 129 F.3d 327, 331 (4th Cir. 1997).

D. The Section 230 Debate Needs More Transparency

I am thrilled to see Section 230 suddenly receiving much-deserved attention, as it is one of the most important technology-related laws in the United States. Unfortunately, some of this attention has lacked precision and accuracy. This is due to a number of problems, including the nuances of Internet liability law and what I imagine is a substantial amount of lobbying efforts on all sides.

But the debate also is muddled because the general public has little insight into the possibilities—and challenges—of content moderation at scale. Until recently, many large tech companies were not terribly transparent about their policies and practices, though the recent Section 230 debates have had the positive impact of shining a bit of sunlight on content moderation. We need far more. Platforms should continue to provide more information about how and why they moderate content, and the possibilities and limits of human-based and automated moderation. If platforms are not transparent, Congress should consider whether to require or provide incentives for better transparency.

Before we can develop new policies regarding intermediary liability and content moderation, we need a more robust factual record. Section 230 is too important to overhaul in the dark. Last October, I suggested the creation of a congressionally chartered commission to gather facts and recommend a path forward.[43] The commission would have a wide range of stakeholders, including civil liberties groups, victims' advocates, law enforcement, and technology companies and their counsel. The Cyberspace Solarium Commission provides a good model for a bipartisan group of experts who gather facts and develop well-reasoned proposals.

A commission also could help to better identify the goals of Section 230 reform and sort through the many current calls for reform, some of which conflict with one another. The criticisms of platforms vary widely, with some arguing that platforms do not moderate enough, and others arguing that they moderate too much, at least for certain political viewpoints. It is difficult to reconcile these criticisms, let alone modify Section 230 in a manner that satisfies of them. Before we identify a solution, we must agree on a problem.

* * *

I commend the Chairman and Ranking Member for the thoughtful solutions that you propose in the Platform Accountability and Consumer Transparency Act. The legislation addresses the need for more transparency in content moderation policies and procedures, and begins the process of identifying the most tailored and reasonable rules for providing that transparency. The bill also provides people with a mechanism to take down material that has been adjudicated to be defamatory or illegal under Federal criminal or civil law. In my experience, plaintiffs who are the victims of the most harmful defamation campaigns are most interested in having the material removed rather than recovering damages, and this legislation provides them with an avenue. We must ensure that a take-down provision is not abused—for example, via the falsification of court orders—but it also is important to allow for the removal of material that is adjudicated to be illegal.

As I routinely remind technology companies, Section 230 is not set in stone, and can be repealed or significantly amended as easily as it was passed. Congress may determine that it is in the public interest to curtail some or all of Section 230s protections. I urge you to make any such decisions with great care.

You likely will hear from many sides of the Section 230 debate about the consequences of your action or inaction. They likely will inform you of these consequences with great certainty. As I have outlined today, there are many reasons to be uncertain about the precise impacts of changes to Section 230. The best that we can do is identify the problems, gather as much information as possible, and address these problems in a focused and tailored manner.

Our online ecosystem relies on these 26 words. As I write in my book, our modern Internet is a house that is "built on the foundation of Section 230." It is difficult to imagine how some of Silicon Valley's largest companies could have emerged—at least in their current forms—without Section 230. The challenge for all of us is to determine how we want the Internet to look over the next 25 years and what it takes to get it.

Senator THUNE. Thank you, Mr. Kosseff.

Next up is Ms. Elizabeth Banker.

[43] Jeff Kosseff, *Understand the Internet's Most Important Law Before Changing It,* REGULATORY REVIEW (Oct. 10, 2019).

Please proceed.

STATEMENT OF ELIZABETH BANKER,
DEPUTY GENERAL COUNSEL, INTERNET ASSOCIATION

Ms. BANKER. Chairman Thune, Ranking Member Schatz, and members of the Subcommittee, thank you for inviting me to testify at this important hearing.

My name is Elizabeth Banker, and I'm Internet Association's Deputy General Counsel.

IA is grateful for the opportunity to appear before the Subcommittee to discuss Section 230, the foundational law that empowers the modern Internet. We appreciate the Subcommittee's thoughtful approach to understanding the history and purpose of Section 230.

IA also appreciates the focus on the twin goals of promoting transparency and accountability in content moderation that are at the heart of the PACT Act.

While we have feedback on the bill, it demonstrates that not all problems related to online content can, or must, be solved by amending Section 230. IA hopes to continue our work with the authors to ensure that the bill can achieve its objectives without hindering innovation and flexibility in content moderation.

Section 230 empowers companies to offer innovative services while simultaneously setting and enforcing policies for using those services. The law carefully balances free expression and protecting consumers in a way that serves their users and their service, and also allowing them to respond to an ever-changing set of challenges. Without Section 230, many individuals and organizations would not be able to create spaces for discussion, because of potential liability for every post.

Section 230 removes disincentives for companies to set and enforce rules for the vast amount of content disseminated on their platforms. As panelists have explained, Section 230 resolves what is called the "moderator's dilemma," allowing Internet companies to adopt and enforce community standards without the fear that it will expose them to unnecessary and often baseless lawsuits. IA members do exactly that, they set and enforce rules for their services, working continually to make them safer. From child sexual abuse material to terrorist content, from self-harm to targeted harassment, IA members have long track records of resource-intensive efforts to combat objectionable online content and providing tools to allow their users to control their online experiences.

Our member companies are constantly learning and adapting their approaches to strike the appropriate balance between allowing expression and protecting users. It's not easy, and such action is frequently subject to criticism from all sides, concerned either that too much or too little has been done.

Spam is a helpful example of how Section 230 works. Providers must continually adjust their enforcement efforts in realtime as spammers adopt new techniques designed to evade detection. The scale of these efforts is staggering. Facebook took action against 1.9 billion pieces of spam in a 3-month period. In multiple cases, Section 230 has shielded providers from lawsuits from spammers who sued over removing their spam material. And the courts have ap-

plied Section 230 and allowed the valuable work that the companies do to continue.

To better understand how the law works more broadly, IA reviewed over 500 decisions involving Section 230. While the national policy debate is focused on a few extreme examples that break into national media or specific content moderation decisions, the importance of Section 230 is best demonstrated by the lesser-known cases that escape the headlines. These cases show that the law continues to perform as Congress intended, quietly protecting discussion boards operated by soccer parents, nurses, police associations, and labor union members, protecting them from lawsuits.

When applied by courts, Section 230 is far from a blanket immunity. Only 42 percent of the decisions we reviewed relied primarily on Section 230. Over a quarter of the decisions involved claims that were dismissed for case defects that were separate and apart from Section 230. Courts rejected Section 230 defenses when they did not apply. Further, courts looked carefully at the provider's role in creating content, a determining factor on whether or not Section 230 applies, frequently requiring further investigation before making a decision. Ultimately, our study supports the call for a thorough and unbiased review of 230 to determine what, if any, changes are necessary before legislating.

Great care should be taken when considering possible changes to Section 230 or legislating on content moderation, given the ever-evolving nature of Internet technology and the complexity of law surrounding online speech.

Thank you. I look forward to your questions.

[The prepared statement of Ms. Banker follows:]

PREPARED STATEMENT OF ELIZABETH BANKER, DEPUTY GENERAL COUNSEL, INTERNET ASSOCIATION

Chairman Thune, Ranking Member Schatz, and members of the Subcommittee, thank you for inviting me to testify at this important hearing today. My name is Elizabeth Banker, and I am Deputy General Counsel of Internet Association.

Internet Association is grateful for the opportunity to appear before this Subcommittee to discuss Section 230—the foundational law that has fostered the development and growth of the variety of online services that consumers consider the best of the internet. We appreciate the Subcommittee's thoughtful approach to understanding the history and purpose of Section 230, and I hope my testimony will assist in your efforts.

IA is the only trade association that exclusively represents leading global Internet companies on matters of public policy. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. IA believes the Internet creates unprecedented benefits for society, and as the voice of the world's leading Internet companies, IA works to ensure policymakers and other stakeholders understand these benefits.

Section 230 plays a critical role in empowering companies to offer innovative services and set and enforce policies regarding the use of those services. IA hopes, through our testimony, to explain: (1) how Section 230 enables our members' services by allowing them to take action against harmful activity when they find it; (2) how the law strikes a careful balance by barring certain types of lawsuits and encouraging moderation; (3) the role of the First Amendment in this debate; and (4) considerations for policymakers looking at possible amendments to Section 230 including IA's preliminary thoughts on the PACT Act. This testimony also provides new research, based on our analysis of more than 500 court decisions involving Section 230, that sheds light on the wide variety of parties using the law, how the law affects litigation, and how courts apply it.

Many of the things people consider to be the "best of internet" are possible because of Section 230. IA's research shows that consumers value hearing from other consumers about their experiences before making major purchases, booking travel,

and ordering a ride-share.[1] Consumers check online reviews more frequently than recommendations from experts or friends. Section 230 allows users to access and share a wide range of information, opinions, and experiences. This type of sharing is at the core of many IA members' services and is what makes them enjoyable, useful, and engaging for their users. It is difficult to imagine a world where all of that would be possible if, for example, a travel site could be held legally responsible for every word in every review it hosts.

IA member companies recognize that in order to realize the full benefits of the internet, it is critical that they take action to prevent and respond to harmful online activities. This is essential to building and maintaining both user and public trust. Today's world, where we grapple with a global pandemic and a social justice movement that is a reckoning with lives lost to systemic discrimination, has shown both the tangible benefits of online services and the critical role providers play in ensuring that their services are not undermined and misused in ways that threaten individual lives or the public good.

IA members have played an essential role in helping society transition into today's "new normal." Their services allow us to stay connected to loved ones, order takeout to support local restaurants, conduct doctors' appointments via telehealth services, and even work from home through video conferences.

While IA's members recognize that their platforms always have room for improvement, they are consistently working to find ways to make their services safer—whether by highlighting authoritative sources of accurate information about COVID–19 and addressing dangerous misinformation, or by working to make underrepresented and marginalized groups feel that they have a safe place to express themselves. Many of our members have made commitments as a result of recent events to do more, and IA as an organization is also actively working to support these efforts. IA has centralized and detailed member company efforts in response to COVID–19 as a resource for the public and policymakers.[2] As part of its commitment to social justice, IA is building on the work in its 2019 Diversity & Inclusion Benchmark Report; helping underrepresented groups find employment opportunities with technology companies through a soon-to-be-launched job portal; and supporting social justice reform legislation.

I. Section 230 Is Critical To Content Moderation And Content Moderation Is Critical To Realizing The Value Of Online Services

In considering possible amendments to Section 230, it is vital to remember the statute's history. Congress enacted Section 230, in part, to encourage providers of online services to voluntarily adopt robust content moderation policies and practices. Congress was reacting to two lower court cases, *Cubby, Inc. v. CompuServe Inc.,* 776 F. Supp. 135 (S.D.N.Y. 1991), and *Stratton Oakmont, Inc. v. Prodigy Services Co.,* 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). Together, *Cubby* and *Stratton Oakmont* created a powerful disincentive for Internet companies to monitor and remove objectionable content by threatening to expose companies to burdensome litigation and potential liability based on their very efforts to moderate that content.[3]

Before the enactment of Section 230, these cases presented Internet companies with a difficult choice. If they voluntarily adopted content moderation policies and practices, they could end up like Prodigy—treated as a "publisher" that could be held liable for user-generated content. But if they sought to avoid this liability as CompuServe had, they would be forced to take a hands-off approach and bury their

---

[1] Internet Association, Best of the Internet Survey, June 26,2019. Available at: *https://internetassociation.org/publications/best-of-the-internet-survey/*.

[2] *https://covid19.internetassociation.org/industry/response/*.

[3] In *Cubby,* a Federal district court held that an interactive service provider, CompuServe, could not be held liable for allegedly false statements that a third-party had posted in one of its online forums unless CompuServe knew or had reason to know of the allegedly false statements. 776 F. Supp. at 139–141. The plaintiffs had sought to hold CompuServe liable for allegedly false and defamatory statements contained in a third party's daily newsletter that CompuServe hosted. *Id.* at 137, 140. The court noted that it would hardly be feasible "for CompuServe to examine every publication it carries for potentially defamatory statements." *Id.* at 140. In granting CompuServe's motion for summary judgment, the court analogized CompuServe to distributors of third-party content such as bookstores and newsstands. *Id.* The court explained that the requirement that such distributors "must have knowledge of the contents of a publication before liability can be imposed for distributing that publication is deeply rooted in the First Amendment." It therefore concluded that CompuServe could not be held liable unless it knew or had reason to know of the allegedly false statements. *Id.* at 140–141. Given the facts of the case—including that CompuServe exercised "little or no editorial control" over the third-party content available on its platform—the court held that the plaintiffs had failed to set forth sufficient evidence that CompuServe had the requisite knowledge, and the court thus granted CompuServe summary judgment. *Id.*

heads in the sand in an attempt to avoid acquiring knowledge of objectionable third-party content. This dilemma is exacerbated by the immense and rapidly increasing volume of third-party content that online platforms host and are used to disseminate, which makes detecting objectionable content exponentially more difficult. Pre-publication review cannot be scaled to match the rate at which new content is posted, and consequently, requiring it would undermine the core value of these real-time, interactive services.

By contrast, in *Stratton Oakmont,* a New York state court held that the interactive service provider Prodigy could be held liable for allegedly defamatory statements posted on its message boards because it employed staff and used software to monitor and police content in order to attain a reputation as a "family oriented" service. 1995 WL 323710, at *2–4. The court agreed with the conclusion in *Cubby* that mere "distributors" may be liable for defamatory statements of others only if they knew or had reason to know of the defamatory statements at issue. *Id.* But the court concluded that Prodigy was instead a "publisher," liable as if it had itself made the statements, because the court viewed Prodigy as analogous to a newspaper that is "more than a passive receptacle or conduit for news, comment and advertising." *Id.* As a result, the court ruled Prodigy could be held liable for defamatory content posted on its message boards even if it lacked knowledge of that content. *Id.* The key distinction, according to the court, was that unlike CompuServe, Prodigy "held itself out as an online service that exercised editorial control over the content of messages" on its platform. *Id.*

Section 230 provides a thoughtful solution to the so-called "moderator's dilemma." It allows Internet companies to adopt and enforce community standards without the fear that doing so would expose them to an onslaught of burdensome lawsuits. In this way, Section 230 creates critical breathing room for online providers to voluntarily undertake moderation of the unprecedented stream of content that users disseminate through their platforms. It creates a middle ground between the wild west of completely passive platforms and the closed-to-the-public realm of newspapers and other media outlets that develop and/or hand-select content for publication. That is why the statute plays such a critical role in ensuring that companies of all sizes, including IA's members, can operate the online services that the public finds so valuable.

II. Section 230 Achieves The Careful Balance It Was Designed To Create

Section 230 has been successful in achieving the goals that led to its enactment. IA member companies have adopted and enforced essential content moderation policies, just as Congress intended in enacting Section 230. In numerous areas—from child sexual abuse material (CSAM) to terrorism-related content, and from self-harm to fake reviews—IA member companies have undertaken decades-long and resource-intensive efforts to combat objectionable online content. At the same time, Section 230 has allowed the online economy to develop and prosper in the United States in ways that simply have not been replicated elsewhere around the globe. Section 230 has spurred the vibrant growth of the Internet and a wide variety of diverse platforms, while also permitting Internet companies to protect users, and to promote healthier online discourse, through responsible domestic and international content moderation.

A few examples can illustrate this point.

First, IA member companies take multifaceted approaches to combating CSAM on their services and in the world that are enabled by Section 230. For example, Microsoft donated PhotoDNA, image-matching software that detects CSAM, to the National Center for Missing and Exploited Children (NCMEC), so that it could be licensed for free to other entities to identify versions of previously reported CSAM. The use of existing and newly developed detection tools has significantly increased, as is evidenced by the dramatic growth in the number of CyberTipline reports in recent years. Today, IA member companies, alongside governments, civil society, and other stakeholders, continually work to stop bad actors from spreading CSAM online. They take a variety of actions, including dedicating engineering resources to the development and improvement of tools like PhotoDNA and Google's CSAI Match, assisting in the modernization of the CyberTipline through donations of engineering resources or funds, and engaging with law enforcement agencies. Many companies also proactively detect instances of CSAM and report to NCMEC.

IA member companies have also engaged in serious efforts to eliminate content advocating or promoting terrorism. Twitter suspended 115,861 unique accounts for violations related to the promotion of terrorism during the first half of 2019.[4] Over

[4] Twitter Transparency Report, Jan.–June 2019, Rules Enforcement. Available at: *https://transparency.twitter.com/en/twitter-rules-enforcement.html.*

85 percent of those accounts were flagged by internal tools developed by Twitter itself, and many of the accounts were suspended before they ever issued even a single tweet. In the first quarter of 2020, Facebook took action on 6.3 million pieces of content supporting terrorism, with 99.3 percent of such content internally flagged before a third party reported it.[5] During the same period, YouTube removed 258,908 videos for violating its policies against violent extremism.[6] IA member companies consistently work to quickly remove any content that advocates terrorism.

IA member companies also employ a multitude of general-purpose technologies to support their content moderation efforts. IA members provide "report abuse" buttons and other mechanisms so that users can flag problematic content or contact the companies with complaints. The companies also provide specific community guidelines that provide standards for third-party content, and they devote significant staff and resources to enforcing those policies. Broad collaboration with civil society groups and other experts informs and deepens our members' commitment to safety and security. In addition, the companies have developed sophisticated software and algorithms to detect and remove harmful content. In many instances, they have shared these technologies to help others eradicate that harmful content as well. Some companies also dedicate large teams of staff that can provide quick responses to evolving problems, including responding to user complaints and removing objectionable and unlawful content. These efforts are the types of activities that Section 230 was designed to promote. It is because of, not in spite of, the law that IA members are able to take action to create safe experiences for their users.

Section 230 has played a particularly important role in creating space for online platforms to refine their approaches to content moderation over time. Moderating content is not easy given the enormous volume of content online and the sometimes-nuanced distinctions that platforms must make to strike the right balance between which content to remove and which to leave up. Our member companies recognize that they do not always achieve the perfect balance, but they are constantly learning, adapting, and updating their approaches.

Section 230 allows online companies the room to experiment in this way without having to worry that they will face the heavy costs of litigation each time a mistake is made or someone is unhappy with a moderation decision. Companies can learn and make adjustments—an essential process that they engage in constantly.

The difficulty of content moderation and the importance of Section 230 is best demonstrated using an example of content that is universally hated—spam. Since the advent of the commercial internet, spammers have been intent on finding ways to flood online services with unwanted commercial messages. Their business is one of volume—if enough messages go out, even if only a small percentage are acted upon, it is profitable. The high volumes of spam messages can operate as a literal or figurative "denial of service attack." They can choke capacity of even large providers and render services of minimal value to their users by obscuring the content users want to see. It is for these reasons that spam was among the earliest targets of proactive content moderation efforts and exemplifies the challenges providers face in keeping pace with bad actors who are determined to misuse their services.

Spam detection has evolved over time from simple techniques, such as spam block lists and rate limiting on accounts to prevent any one account from sending too many messages at once, into something altogether more sophisticated. While many of the early techniques remain important tools, new algorithmic approaches that pull signals from a variety of sources are essential today. These more sophisticated tools are able to assign risk based on numerous indicators and then apply any one of a variety of interventions, including pausing account activity, requiring further account verification or passing reCaptchas to verify it is not automated activity, demoting suspect content, blocking or deleting content, and closing accounts of violators. The battle between spammers and service providers can be characterized as an arms race, as spammers quickly adapt to detection techniques and providers must continually respond. The automated systems that protect providers' services from spam may be changed on a daily, if not a more frequent, basis.

The volume of spam activity actioned by IA members is staggering. For example:

---

[5] Facebook Transparency, Community Standards Enforcement Report. Available at: *https://transparency.facebook.com/community-standards-enforcement#dangerous-organizations.*

[6] Google Transparency Report, YouTube Community Guidelines Enforcement, Video Removals by Reason. Available at: *https://transparencyreport.google.com/youtube-policy/removals?hl=en&total_removed_videos=period:Y2020Q1;exclude_automated:human_only&lu=total_removed_videos.*

- Facebook: In the three-month period from July to September 2019, Facebook took action against 1.9 billions pieces of content for spam.[7]
- Twitter: During the first six months of 2019, Twitter received over 3 million user reports of spam and challenged over 97 million suspected spam accounts.[8]
- YouTube: In the first quarter of this year, 87.5 percent of channel removals were for violations that were related to spam, scams, and other misleading content resulting in 1.7 million channels being removed. In addition, in the same period, YouTube removed over 470 million spam comments.[9]

Section 230 is critical to these content moderation efforts. Indeed, service providers sued by spammers for removing spam have asserted Section 230 as a defense.[10] Section 230 is even more critical to efforts to address content for which there is no general global agreement that it is harmful or should be restricted. Providers develop policies across a range of issues that are extremely nuanced and uniquely tailored to their services, addressing a broad range of behaviors that are disruptive to the goal of the service they provide. There are frequently contrasting views about whether individual content moderation decisions were correct or flawed. No single solution could ever balance all of the competing visions of how content moderation ought to work. Instead, Section 230 protects a critical equilibrium that safeguards free expression and promotes user safety, while allowing providers the flexibility to respond to an ever-changing landscape of challenges in a way that best serves their users and their unique services.

III. IA's Review of Section 230 Decisions

Over a year ago, IA began reviewing court decisions involving Section 230 with a goal of developing a better understanding of how the law works in practice. Having now reviewed more than 500 decisions, IA is sharing its observations which demonstrate the need for in-depth study of this case law to inform the public policy debate over Section 230. In recent years, the national policy debate around Section 230 has focused on a few cases that garnered national media attention or specific content moderation decisions by particular providers. Employing a holistic approach will ensure that all stakeholders have a comprehensive understanding of Section 230 before advocating for changes to the careful balance that it strikes.

IA's findings are further described in the attached paper, along with a description of our methodology and the list of decisions reviewed. IA acknowledges that the review was not comprehensive and that there are inherent limitations in attempting to draw broad characterizations from the outcome of any stage in litigation. However, we found clear patterns and observations of important note for policymakers based on judicial decisions reviewed where Section 230 immunity was implicated. IA believes that this initial effort provides a sufficient basis to support a call for a comprehensive and unbiased review of Section 230 before any action is taken to change the law. I would like to share some of our observations with you today.

A. Section 230 Benefits A Wide Range Of Entities.

IA's review of Section 230 decisions revealed that it is not only large social media companies that assert Section 230 as an affirmative defense. The importance of Section 230 is best demonstrated by the lesser-known cases that escape the headlines. Online users; Internet service providers and website hosts; online newspapers; universities; libraries; search engines; employers; bloggers, website moderators and listserv owners; marketplaces; app stores; spam protection and anti-fraud tools; and domain name registrars have all asserted Section 230 immunity. These decisions show the law quietly protecting soccer parents from defamation claims, discussion boards for nurses and police from nuisance suits, and local newspapers from liability for comments posted by trolls.

It is critical to keep these smaller entities in mind when evaluating the value of Section 230. For example, in *Joyner v. Lazzareschi,*[11] Lazzareschi, a soccer parent and the operator of a local online messaging board for youth soccer called SoCalSoccerTalk, was sued by Joyner, a disgruntled soccer coach, for allegedly defamatory comments that parents made on the regional messaging board. While Lazzareschi would have fallen under the Section 230 definition of a "provider" of an "interactive computer service", the case was ultimately dismissed and the decision was upheld on appeal for Joyner's failure to meet the requirements for a defamation

[7] Facebook Transparency Report, n. 5.
[8] Twitter Transparency Report, n. 4.
[9] Google Transparency Report, n. 6.
[10] *See, infra,* fn. 16.
[11] No. G040323, (Cal. App Jul 10, 2012).

claim. Another example of a lesser-known entity to assert Section 230 is Allnurses.com, in the case of *East Coast Test Prep LLC v. Allnurses.com Inc.*[12] In this case, Allnurses.com, was sued by East Coast Test Prep (ECTP) because two nurses made negative remarks about ECTP's services. While this case was dismissed at the summary judgment phase for a variety of shortcomings in the plaintiff's case, Allnurses.com also successfully argued that Section 230 protected its service from liability for allegedly defamatory statements made by the nurses that used their message board to discuss topics important to the nursing field, including the relative merits of test prep providers. It is these small fora and communities, local soccer messaging boards and discussions of nursing exam courses, that would be silenced by crippling litigation without Section 230.

These examples represent just two of the seldom discussed entities that are among the wide-cross section of Section 230 beneficiaries. They are joined by local newspapers, labor unions, police associations, individuals, and others who provide spaces for users to discuss topics of interest. These entities and individuals make important contributions to the online ecosystem that exists today. During the pandemic, many of these online communities that support sharing of hyperlocal information, like the length of the line at the local COVID testing site, the health and safety measures employed by a favorite neighborhood restaurant, or resources for assistance such as food banks, play a critical role in helping us cope and recover. It is important for this Subcommittee to keep in mind the impact that changing Section 230 may have on a variety of entities and individuals within the online platform space.

B. Courts Dismiss Many Cases In Which Section 230 Is Raised As A Defense Based On Unrelated Defects In Plaintiffs' Claims.

Our review found that Section 230 is far from a "blanket immunity"[13] when it comes to the law's application in the courts. Instead our research demonstrates that only 42 percent of decisions reviewed were decided primarily based on Section 230 immunity. In over a quarter of the decisions (28 percent), the courts dismissed claims without relying on Section 230 because the plaintiff failed to state a claim upon which relief could be granted, or because of other defects in their case. Courts rejected attempts to rely on Section 230 when it was not applicable—whether because the party asserting 230 was not a covered entity, an exception applied, or the party asserting 230 was a content provider of the information at issue. Courts carefully consider the issue of the service provider's role in the creation of the problematic content, a determining factor on whether Section 230 applies.[14] When rejecting complaints based on Section 230, judges frequently explained in detail the requirements to adequately allege that the provider developed—in whole or in part—the content at issue, and gave plaintiffs multiple tries to amend their complaints. When plaintiffs did raise factual issues as to the service provider's role in content development, courts required discovery to allow further investigation before rendering a judgment as to whether Section 230 applied.[15]

C. Section 230 Protects Providers Who Engage in Content Moderation, But Typically Through The Application Of Section 230(c)(1)'s "Interactive Computer Service" Provision Not Section 230(c)(2)'s "Good Samaritan" Provision.

In our review, only 19 of the 516 court decisions in which Section 230 was raised as a defense were resolved on the basis of Section 230s (c)(2) "good Samaritan" clause, which provides immunity for actions taken "voluntarily" in "good faith" to restrict content that is "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." Furthermore, the majority of these cases in-

---

[12] No. Civ. 15–3705 (JRT/SER), (D. Minn. Jan 26, 2018).

[13] *See, e.g.,* Executive Order on Preventing Online Censorship, May 28, 2020. Available at: *https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/;* Department Of Justice's Review Of Section 230 Of The Communications Decency Act Of 1996, at 4(a). Available at: *https://www.justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996?utm_medium=e-mail&utm_source=govdelivery.*

[14] *See, e.g., Enigma Software Group v. Bleeping Computer,* 194 F. Supp. 3d 263 (2016); *Tanisha Systems 3v. Chandra,* 2015 U.S. Dist. LEXIS 177164 (N.D. Ga. 2015); *Perkins v. LinkedIn,* 53 F. Supp. 3d 1222 (2014); *Brummer v. Wey,* 2016 NY Slip Op 31021(U); *Dimetriades v. Yelp,* 228 Cal. App. 4th 294 (2014).

[15] *See, e.g., General Steel v. Chumley,* 840 F.3d 1178 (10th Cir. 2016); *Samsel v. DeSoto County School District,* 242 F.Supp.3d 496 (N.D. Miss. 2017); *Pirozzi v. Apple,* 913 F. Supp. 2d 840 (N.D. Cal. 2012); *Cornelius v. Delca,* 709 F. Supp. 2d 1003 (D. Idaho 2010); *Best Western v. Furber,* No. CV–06–1537–PHX–DGC (D. Ariz. September 5, 2008); *Energy Automation Systems v. Xcentric Ventures,* Case No. 3:06–1079 (M.D. Tenn. May. 25, 2007); *Hy Cite v. Badbusinessbureau.com,* 418 F .Supp. 2d 1142 (D. Ariz. 2005).

volved provider efforts to block spam.[16] In other such decisions, courts resolved claims based on Section 230(c)(1),[17] Anti-SLAPP motions,[18] the First Amendment,[19] or for failure to state a claim or other deficiencies.[20]

Another reason (c)(2) has not been invoked more often is that, when providers are sued for removing content, many of those lawsuits are based on assertions that the provider has violated the First Amendment rights of the user whose content was removed.[21] As the First Amendment applies to only government actors, these cases have been dismissed for failure to state a claim without the necessity of defendants asserting or a court analyzing Section 230. In fact, courts have found that service providers' decisions regarding whether and how to display content are protected by the First Amendment.

IV. Considerations For Policymakers

It is of the utmost importance that policymakers tread carefully when considering possible changes to Section 230 or enacting any other laws targeting content moderation. This caution is necessary because of the ever-evolving nature of harmful content and Internet technology, as well as the complexity and variety of potential legal liability for online speech. This caution is also essential in light of foundational First Amendment principles.

A. Maintaining The Careful Balance Struck By Section 230.

Section 230, in its current form, supports a diverse Internet ecosystem that provides users with reviews, places for discussion and lively debate, and opportunities to expand their knowledge. Without Section 230s protection, Internet companies would be left with a strong disincentive to monitor and moderate content. Section 230 removes this disincentive to self-regulate, creating essential breathing space for Internet companies to adopt policies and deploy technologies to identify and combat objectionable or unlawful content—or to develop other innovative solutions to address such content. Society benefits from the rules that providers voluntarily set and enforce to enhance user experiences as well as safety, goals that would be challenging—if not impossible—for the government to achieve directly due to the First Amendment. Through exceptions and carefully crafted language limiting Section 230s protections to only third-party content and activities, bad actors can still be held accountable when they participate in, or materially contribute to, illegality.[22] Over the more than two decades since Section 230s enactment, the Internet continues to thrive due to the carefully crafted language balancing the fostering of online innovation with ensuring there are proper ways to hold content providers accountable for their actions.

B. Ensuring That Any New Requirements Recognize The Flexibility Required For Effective Content Moderation.

Some proposals to change Section 230 have the potential to impact how service providers conduct content moderation by limiting the protections in the statute to just certain types of content, or setting new rules for how companies engage in content moderation activities. Policymakers considering making changes to Section 230 must recognize the wide cross-section of online services that rely on the law and keep in mind the need for flexible and non-prescriptive language. There are important reasons why the broad group of entities and individuals who qualify as providers of interactive computer services should be able to retain discretion and flexibility to set and enforce their rules. For example, content moderation teams should

---

[16] *See. e.g., Holomaxx Technologies Corp. v. Yahoo!, Inc.,* No. 10-cv-04926 JF (PSG) (N.D. Cal. August 23, 2011), *E360INSIGHT, LLC v. Comcast Corp.,* 546 F.Supp.2d 605 (N.D. Ill. 2008); *Pallorium v. Jared,* G036124 (Cal. Ct. App. Jan. 11, 2007); *America Online, Inc. v. GreatDeals. Net,* 49 F. Supp. 2d 851 (E.D. Va. 1999).

[17] *See, e.g., DeLima v. YouTube,* 2019 WL 1620756 (1st Cir. Apr. 3, 2019); *Green v. AOL,* 318 F.3d 465 (3d Cir. 2003); *King v. Facebook,* 3:19-cv-01987 (N.D.Cal. Sept 5, 2019).

[18] *See, e.g., Sikhs for Justice v. Facebook,* 144 F. Supp. 3d 1088 (N.D.Cal. 2015); *Johnson v. Twitter,* No. 18CECG00078 (Cal. Superior Ct. June 6, 2018).

[19] *See, e.g., Davison v. Facebook,* 370 F. Supp. 3d 621 (E.D. Va. 2019); *Estavillo v. Sony Computer Entm't Am.,* 2009 WL 3072887 (N.D. Cal. Sept. 2, 2009).

[20] *See, e.g., Roberson v. YouTube,* 2018 DNH 117 (D. N.H. 2018); *Young v. Facebook,* 790 F. Supp. 2d 1110 (N.D. Cal. 2011); *Lewis v. YouTube,* No.H041127 (Cal. App. January 25, 2016)

[21] *See, e.g., Tulsi Now, Inc. v. Google, LLC; Prager University v. Google LLC,* 951 F.3d 991 (9th Cir. 2020); *amango v. Facebook, Inc.,* No. 3:11–CV–0435, 2011 WL 1899561 (N.D. NY April 19, 2011); *Davison v. Facebook, Inc.,* 370 F.Supp.3d 621 (E.D. Va. 2019); *Federal Agency of News LLC v. Facebook, Inc.,* 2020 WL 137154 (N.D. Cal. Jan. 13, 2020; *Zhang v. Baidu. com Inc.,* 932 F. Supp. 2d 561 (S.D.N.Y. 2013); *Buza v. Yahoo!, Inc.,,* No. C 11–4422 RS (N.D. Cal. 2011).

[22] *Fair Housing Council of San Fernando Valley v. Roommate.com,* 521 F.3d 1157, 1168 (9th Cir. 2008) (*en banc*). In addition, Section 230(e) outlines the criminal law, intellectual property, state law, communications privacy law, and sex trafficking law exemptions from 230 immunity.

be encouraged to be nimble enough to respond to unanticipated events quickly. The urgent nature of the response to the video of the Christchurch attack is a good example of how world events can impact content moderation efforts. The circumstances of the Christchurch attack are precisely why providers need to be able to make adjustments to the techniques they use to battle policy violations to adapt alongside the ever-evolving nature of threats. Imposing overly prescriptive and burdensome requirements through legislation or regulations will negatively impact the Internet ecosystem. Without flexibility, service providers are unable to effectively moderate content on their platforms, which could dramatically reduce the quality of their services. Furthermore, online platforms are not uniform in their breadth, construction, business models, or approach to content hosting. Changes to Section 230 intended to address concerns with a particular platform or type of platform, will impact all platforms. Given the discrete but important differences among Internet platforms, changes to Section 230 must carefully consider the broad and varied impacts of legislative language on different platform models.

C. Aligning With Established First Amendment Principles That Apply To Content Moderation.

Any amendments to Section 230, and any other laws pertaining to content moderation, should take careful account of three First Amendment guardrails.

First, platforms are not state actors and consequently need not refrain from moderating speech protected by the First Amendment. The First Amendment only limits the actions of state actors—that is, governmental entities—not private companies merely because those companies provide forums for speech. Courts have consistently held that Internet platforms are not state actors bound to follow the strictures of the First Amendment.[23] Plaintiffs cannot bring suit against platforms alleging that the platforms somehow violated the plaintiffs' right to express particular speech under the First Amendment. Some have suggested that social media sites should be treated as public forums subject to First Amendment restrictions. However, most users would not want the First Amendment to dictate Internet platforms' content moderation practices as though they were state actors. If that were to happen, platforms would be prevented from blocking or screening a wide-range of problematic content that courts have held to be constitutionally protected including pornography, hate speech, and depictions of violence.

Second, the First Amendment protects the rights of the platforms themselves. When platforms determine what kind of platform to be and what kinds of content to host or prohibit, those are forms of free expression protected by the First Amendment. It is bedrock First Amendment doctrine that such editorial decision-making is constitutionally protected. In *Miami Herald Publishing Co. v. Tornillo,*[24] for instance, the Supreme Court held that a statute requiring newspapers to provide political candidates with a right of reply to critical editorials violated the newspaper's First Amendment right to exercise "editorial control and judgment" in deciding the "content of the paper."[25] Several courts have applied this reasoning in the online context, holding that platforms possess the First Amendment right to decide what content to carry.[26] Recognizing this principle has never been more important. It is critical to allowing online communities and services to develop around common interests, shared beliefs, and specific purposes. It is also critical to allowing online services to cater to different audiences, including the ability to design rules to make their services age-appropriate or purpose-appropriate.

Third, the First Amendment sets a constitutional floor that ensures that online platforms that carry vast quantities of third-party content cannot be held liable for harms arising from that content based on a standard of strict liability or mere negligence. Applying such non-protective standards of liability to entities that distribute large volumes of third-party material would violate bedrock First Amendment principles. The Supreme Court examined this issue over six decades ago, in *Smith v. California.*[27] There, a city ordinance prohibited bookstores from selling obscene or indecent books regardless of whether the store owners knew the books were obscene or indecent.[28] The ordinance violated the First Amendment, the Court explained, because it would cause a bookseller to "restrict the books he sells to those he has inspected" and thus "impose a severe limitation on the public's access to constitu-

---

[23] *See, e.g., Freedom Watch, Inc. v. Google Inc.,* 2020 WL 3096365, at *1 (D.C. Cir. May 27, 2020) (per curiam); *Prager Univ. v. Google LLC,* 951 F.3d 991, 996–999 (9th Cir. 2020).

[24] 418 U.S. 241 (1974).

[25] *Id.* at 258.

[26] *See, e.g., Jian Zhang v. Baidu.com Inc.,* 10 F. Supp. 3d 433, 436–443 (S.D.N.Y. 2014); *Langdon v. Google, Inc.,* 474 F. Supp. 2d 622, 629–630 (D. Del. 2007).

[27] 361 U.S. 147 (1959).

[28] *Id.* at 148–149.

tionally protected matter."[29] This principle—that the First Amendment gives special protection to those who act as clearinghouses for large quantities of third-party content—applies with especially great force to Internet platforms, given the exponentially greater volumes of content that they host and the important role they play in societal discourse. Were these platforms to face liability for distributing unlawful third-party material absent circumstances in which they both knew of that particular content and yet failed to remove it, Internet users' access to vital constitutionally protected speech would be severely stifled.

This trio of First Amendment principles provides important constitutional guardrails that protect free expression on the internet. Along with Section 230, they have contributed to making the Internet a vibrant medium that benefits so many. Policymakers addressing content moderation must therefore carefully consider the interaction between these principles and new policies before enacting new laws that could threaten to undermine the constitutional foundation of our dynamic internet.

V. The PACT Act

Given the many crucial considerations implicated by any proposal to amend Section 230, IA appreciates the thoughtful approach taken by Senators Schatz and Thune in the "Platform Accountability and Consumer Transparency Act" or the "PACT Act." IA and its member companies appreciate the focus in the bill on the twin goals of promoting transparency and accountability in content moderation. Over the last several years, IA member companies have been working continuously to enhance transparency with their users and the public about their community rules; how they are enforced; and how often they are enforced. These efforts include expanding transparency reporting to cover a wider range of topics including content removals for terms of service violations, making the rules of the service easier to understand and more detailed, providing additional user education and guidance through examples of potential rule violations, and explaining in more detail how rules are enforced and the potential consequences for violations. These efforts are just one part of how IA member companies approach content moderation and supplement measures such as easy reporting of violating content, user notices and appeals, and proactive efforts to find violating content. The PACT Act's focus on these aspects of content moderation in many ways align with IA member company efforts, and for that reason, IA hopes to work with the sponsors to ensure that the bill is able to achieve its goals without inhibiting flexibility and innovation in content moderation.

IA would like to highlight two areas of concern related to the bill's broad scope and highly detailed requirements. With regard to the bill's scope, the requirements for transparency and accountability in Section 5, as drafted, would apply to all "interactive computer services" (ICSs), which is essentially the same group of entities that benefit from the protections of Section 230. As discussed above, Section 230 applies to a wide-range of interactive services and platform models including those offered by individuals, informal clubs or groups, and member associations. In addition, the types of services that fit within the term "interactive computer service" are likewise broad, covering not only social media services, but also private messaging, search, message boards and listservs, dating services, job search platforms, review sites, and more. IA is concerned that the requirements of Section 5 would prove too large a burden for those ICSs as hobbyists, volunteers, and as adjuncts to other activities. Such requirements may force these individuals and entities to shut down their projects and may discourage similarly situated individuals and groups from engaging in important expressive activity. There are also services for which transparency requirements may not make sense given the type of service or the purpose for which it was created. For example, under Section 5, review platforms would have to disclose to fraudsters (*e.g.,* rival businesses or competitors of the business being reviewed) that their fake reviews had been detected and give fraudsters an opportunity to appeal the takedown of their fake review. While transparency is often a benefit, the burdens associated with these particular requirements should be carefully weighed against the benefits they would likely achieve. For this reason, IA hopes to work with the sponsors to consider potential changes to the scope of the bill.

The other potential issue IA would like to share regarding the bill relates to the negative ramifications the highly detailed requirements in Section 5 could have. First, the detailed nature of the requirements would be extremely burdensome for all ICSs, and it would be a struggle for all but the most highly resourced providers to comply. For example, in order to comply with transparency reporting requirements, providers would need to rebuild the systems they use to process and track

[29] *Id.* at 153.

user reports, as well as any systems that operate independently to moderate content, to ensure that all of the required types of information are collected for future reports. Absent a long window to ramp up, providers may need to manually review each individual report to collect information for backwards-looking reports. The difficulty of complying could adversely impact content moderation as providers may choose to narrow their content policies to limit the scope of issues that would have to be addressed by the requirements of Section 5. Therefore, these requirements could unintentionally result in *less* moderation, rather than more.

As with the scope of the bill, the Section 5 requirements would likely limit the diversity and richness of the different types of individuals and entities that are part of the online ecosystem. This in turn would limit consumer choice and access to information. Small providers in particular would feel the impact of these requirements. In addition, the detailed nature of the requirements would significantly diminish the essential flexibility providers have today to constantly adjust their approaches to content moderation to keep pace with bad actors, respond to emergencies, and focus their efforts on the activities that pose the highest risks to users of their services and the public.

IA appreciates the opportunity to discuss the value of Section 230 to the modern Internet and looks forward to continuing these conversations around our concerns and other feedback pertaining to this bill with the members of the Subcommittee.

APPENDIX: Internet Association, *A Review Of Section 230's Meaning & Application Based On More Than 500 Cases* (July 27, 2020).

Senator THUNE. Thank you, Ms. Banker.

Next up is Mr. Sylvain.

Mr. Sylvain, please proceed.

STATEMENT OF OLIVIER SYLVAIN, PROFESSOR, FORDHAM LAW SCHOOL

Mr. SYLVAIN. Thank you, Committee Chairman Wicker, Ranking Member Cantwell, Subcommittee Chairman Thune, Ranking Subcommittee Member Schatz, members of the Senate Subcommittee on Communications, Technology Innovation, and the Internet.

As vexing as the problems posed by Section 230 are, I am honored to discuss potential reforms of the statute with you today. Let me get straight to it.

Section 230 is not adapted to the ways in which many online intermediaries control practically all aspects of consumers' online experiences. The doctrine presumes that any given interactive computer service is no more than a publisher or distributor of user-generated content, unless that service materially contributes to the content at issue. Sir, courts have been generous to intermediaries under this rule, generally dismissing claims before discovery begins. Courts and plaintiffs, accordingly, never really get to learn how implicated intermediaries are in their distribution and targeted delivery of either the user content or data.

The most powerful online intermediaries today are anything but publishers and distributors of user-generated content. They illicit, harvest, sort, and repurpose user posts and personal data to attract and hold consumer attention and, more importantly, to market this valuable data to advertisers. They do this unfettered by law. The result is too often lived harm to the everyday people whom consumer protection and civil rights laws and remedies exist, but, because of the protection, are unavailable.

Recent civil rights litigation against Facebook's Ad Manager provides a vivid example of this unfair and underregulated political economy for user data. The social media giant relies on sophisticated, but imperfect, automated decisionmaking tools to make

sense of the troves of consumer data that it collects. Through these processes, it creates hundreds of new categories in which advertisers may, as they wish, refine campaigns by including or excluding potential recipients across hundreds of dimensions. For example, distributors of Urdu-language music or WNDA gear can target specific audiences by gender, age, ethnicity, and language, to list just a few variables. Facebook generates these categories through automated algorithmic processes. Consumers, meanwhile, generally have no idea where they fall in the scheme. Facebook, for example, does not ask its consumers to identify with any ethnicity, and yet it slots consumers into proxies for these identities.

Here's the rub. Under civil rights law, Congress forbids discrimination in ads on the basis of race, ethnicity, age, and gender in the markets for housing, education, and consumer credit. But, that is exactly what Facebook allowed building managers and employers to do. A series of blockbuster stories by ProPublica in late 2016 revealed that the service-enabled advertisers, to include and exclude consumers by proxies for race and age, and consumers were not the wiser for it, because they do not see each other's news feed.

Soon after the ProPublica stories ran, civil rights groups and aggrieved plaintiffs brought cases against Facebook in civil and in Federal courts across the country. They alleged that the Ad Manager made discrimination in violation of civil rights laws possible. They also asserted that Facebook targeted ads, on behalf of the advertisers, in ways that were discriminatory. Through its lookalike feature, in particular, Facebook replicates any given advertiser's customer list, and, based on that list, delivers the ads far more widely to people who fit the profile. With regards to these recent civil rights cases against Facebook, the lookalike feature entrenched extant disparities at the expense of members of historically marginalized groups. None of this resembles the news groups and bulletin boards that Congress had in mind in 1996.

The social media giant, nevertheless, moved to have these civil rights claims dismissed, pursuant to Section 230, as it routinely and formulaically does in practically all cases. And most of the time, they win. But, here the courts never got a chance to weigh in, because the parties settled in March 2019. Among other things, Facebook agreed to create a new ad portal for housing, employment, and credit markets to protect against unlawful discrimination in those settings. HUD filed a charge against the company soon afterwards. And, as far as I know, that action remains unresolved.

Importantly, however, researchers from Northeastern University, Upturn, and ProPublica late last year found that, in spite of the settlement, Facebook's Ad Manager continues to distribute job ads that discriminate against women and older people at alarming rates. That is, even as Facebook no longer allows advertisers, in the first instance, to use unlawful proxies in hiring, the Ad Manager nevertheless continues to discriminate.

This is just one example in one area of law, but it underscores that Section 230 has done nothing to cultivate any demonstrable urgency about protecting consumers in this setting even as intermediaries milk that data for ad revenue.

The PACT Act is a good start at reform. The one piece I will emphasize here, with the limited time that I have, is the expansion of the exceptions under 230(e) to include civil government agency enforcement. I would like to see this expanded to include claims by private individuals under Federal and State law, but, even in its current form, the bill would allow courts to scrutinize intermediaries' practices more closely. This would be all the more important in cases in which plaintiffs allege that automated decisionmaking systems cause harm. I can see agencies like the FTC and HUD proceeding pursuant to their statutory mandate in this regard.

Much of the PACT Act would represent the sensible reform that would help to vindicate consumer protection, civil rights, and public law protections for everyday people.

Thanks again for the invitation. I look forward to your questions.

[The prepared statement of Mr. Sylvain follows:]

PREPARED STATEMENT OF OLIVIER SYLVAIN, PROFESSOR, FORDHAM LAW SCHOOL

Committee Chairman Wicker, Ranking Member Cantwell, Subcommittee Chairman Thune, Ranking Subcommittee Member Schatz. Members of the Senate Subcommittee on Communications, Technology, Innovation, and the Internet,

Thank you for inviting me to today's hearing about reforming 47 U.S.C. §230. I have been thinking and writing about this provision and its attendant judge-made doctrine for the past few years. I have argued that the law is not adapted to the ways in which online intermediaries today effectively control practically all aspects of consumers' online experiences. The so-called "immunity" under Section 230, developed in the late 1990s, continues to presume that online intermediaries (or "interactive computer services") are no more than than mere publishers or distributors of user-generated content. The courts have read the provision as a shield from liability unless a plaintiff in any given case successfully pleads that a defendant intermediary "materially contributes" to the content at issue.

Pursuant to this standard, courts today have been unwilling to see anything but glaring direct contributions of substantive content as counting as "material contribution." In 2020, this presumption—this benefit of the doubt—makes no sense. The biggest of these companies today design their services to elicit, collect, harvest, sort, analyze, redistribute, and altogether repurpose their consumers' data in service of their business objectives and the interests of the advertisers who have come to rely on them. And they use sophisticated but demonstrably imperfect automated decisionmaking systems to do this. (They actually purport that these systems, even as they structure the entirety of our online experiences, help them to moderate user content.)

None of this—especially the companies' pecuniary designs on user data—resembles the considerations at work when Congress enacted 47 U.S.C. §230. The relatively quaint and romantic motivations of the Usenet newsgroups or AOL bulletin boards were on the minds of legislators or judges in the 1990s. They could not foresee Big Tech's industrial designs on controlling and consolidating information flows to achieve their own commercial objectives.

Nor does the statute's titular claim that online intermediaries' "Protection for 'Good Samaritan' blocking and screening of offensive material" do any real work. One could reasonably read Section 230(c)(2) as the operative "safe harbor" under the statute, in which case courts would only immunize "interactive computer services" that voluntarily take good faith steps to moderate illicit or illegal user-generated content. But, in practice, that is not what defendants, Big Tech companies, or their advocates have asserted. Rather, they have projected 230(c)(1)'s passive-voice and indirect mandate about how providers of "interactive computer services" should be "treated" onto Section 230(c)(2) in ways that effectively overshadow and essentially eliminate the mechanism for courts to consider whether an online intermediary is reasonably trying to moderate content. Because of this doctrine, defendants raise the Section 230 defense at the motion to dismiss phase, well before plaintiffs and courts ever get to find out how implicated intermediaries are in their control and administration of user content or data.

It is time that the law and doctrine reflect our currently reality. This is why I am honored and eager to engage your consideration of the PACT Act and other re-

forms of the statute. For what it is worth, the following are, in reverse chronological order, the recent pieces I have written on the topic:

- *Solve the Underlying Problem: Treat Social Medias as Ad-Driven Companies, Not Speech Platforms,* Knight Foundation (June 16, 2020)
- *Recovering Tech's Humanity,* 119 Columbia Law Review Forum 252 (November 2019)
- *A Watchful Eye on Facebook's Advertising Practices,* N.Y. Times (March 28, 2019)
- *Discriminatory Designs on User Data,* Knight First Amendment Institute "Emerging Threats Series" (April 2018)
- *Intermediary Design Duties,* 50 Connecticut Law Review 203 (March 2018)
- *AOL v. Zeran: The Cyberlibertarian Hack of § 230 Has Run Its Course,* Law.com (November 2017)

My views of the prevailing doctrine precede the emergent *du jour* argument that social media companies have a liberal coastal urban bias. I will answer inquiries from you on this question if you have them, of course, but, at the outset, please know that I do not believe that online intermediaries' editorial moderation decisions are unlawful or even imprudent. As I have written elsewhere, Facebook and Twitter, for example, have sensibly developed tools that enable their users to control the ways in which trolls and bigots slide into online "conversations" and user-groups. They have used their constitutionally protected editorial prerogative to flag user content that they find hateful or dangerously misleading. The principal question I have in this context is whether these efforts are enough, since illegal content and advertisements continue to proliferate on their services.

More pertinently, I believe that framing the question of Section 230 reform in terms of political viewpoint or even free speech obscures what is truly at work: the political economy of online advertising. The biggest and most popular online intermediaries today are not simple "platforms" for user-generated content as much as commercial services for targeted advertising to consumers. These companies design their applications and the automated decisionmaking systems that power them to maximize advertising revenues. Social media companies in particular are keenly committed to designing services and products that keep users viscerally engaged in service of their bottom-line. We are well past the discounts and coupons that retail chains include in their circulars.

The current debate about Section 230 should focus instead on Big Tech's unprecedented power to control consumer behavior. The beneficiaries of the protection under Section 230 are not in the business of promoting free speech as much as designing services that optimize user engagement which, in turn, maximizes the scope and depth of their advertising revenue. They do this more or less unmoored by settled legal conventions because of the broad protection under Section 230, a doctrinal protection that I do not think any other species of company in the United States has ever enjoyed.

To be sure, their pecuniary motivation, unfettered by the threat of liability under the courts' broad reading of the protection under Section 230, has allowed an array of innovative applications for user-generated content to proliferate. But the current legal protection under Section 230 has also cultivated in application developers a cool, above-it-all indifference to (1) public law norms and (2) the immediate lived harms that so much of the content and data that they distribute causes. Dangerously misleading public health related information, disinformation about elections, nonconsensual pornography, and discriminatory advertising, all of which may be illegal in any given circumstance, proliferate still because online intermediaries do not have to bear the responsibility for designing systems that carefully distribute them. The question for you is whether there is something legislation can do to cultivate and engender a demonstrable sense of social responsibility.

If you were to ask me to make any recommendations today about Section 230 reform, it would first be that courts should read the protection for interactive computer services far more carefully than they have. We have seen slow but steady improvement on that front since the Ninth Circuit's decisions in *Fair Housing Council of San Fernando Valley v. Roommates.com* in 2008 and *Barnes v. Yahoo!* in 2009 and, more recently, perhaps, after the Second Circuit's decision last summer in *Oberdorf v. Amazon.* My humble recommendation to courts is that they should be far more searching than they have been in determining whether a defendant interactive computer services' designs materially contribute to the distribution of illegal content. At a minimum, opening the standard up in this way would allow plaintiffs to engage in discovery on colorable claims—a prerogative that litigants in other legislative fields generally have. Today, most Section 230 defenses are decided at the

motion to dismiss, before any discovery can be had. I urge courts to be far more open to the pleaded claims that online intermediaries' designs materially contribute to illegality. But this is for the courts to sort out under current doctrine.

My humble recommendation to you, as legislators, must be different, as you bring a different, more generalizable and prospective institutional authority: the exceptional legal protection that online intermediaries now enjoy under the statute is ripe for narrowing because, today, it directly causes consumer harms and sometimes entrenches racism, misogyny, and discrimination against members of historically marginalized groups. Public laws and regulations exist to protect people from these kinds of injuries. But, because of the prevailing doctrine, the entities most responsible and capable of protecting people bear no legal responsibility to do so.

Thanks again for the generous invitation to testify. I look forward to engaging your questions as best I can.

Senator THUNE. Thank you, Mr. Sylvain.

Well, we'll dive right into questions.

Representative Cox, one of the most common misconceptions about CDA 230 is that it requires platforms to be politically neutral with respect to its content moderation decisions. Does CDA 230 require platforms to be politically neutral? And, if not, why not?

Mr. COX. No, it does not. Section 230 was never meant to require neutrality. To the contrary, the idea is that every website should be free to come up with its own approach, to let 1,000 followers bloom. If it were otherwise, we could imagine, you know, how, you know, very quickly things would not work. The Democratic National Committee could not have its own website. The Republican National Committee could not. It's not a question of everybody having to be neutral. It is, however, important to distinguish that it is possible for websites to decide that they want to have a business model of political neutrality. And when they do so, they can and should be held to that. If they promise this to the public through their terms of service, through their advertising, through their, you know, rules of content moderation that are published, that "We will do this," then, you know, by all means, hold them to it. And I think, you know, many existing laws are available for this purpose, including the Federal Trade Commission Act and the little FTC Acts in all of the States. There is a well-known case in the Ninth Circuit that used the common law promissory estoppel to require Yahoo! to honor promises to take down material. And so, it is in this framework that I think we should look at political neutrality. If these platforms are holding themselves out as neutral, then they should be held accountable.

Senator THUNE. For those who are concerned about systemic viewpoint discrimination by the content moderation decisions of platforms, wouldn't rigorous transparency requirements for platforms help to reveal whether there is, in fact, systemic viewpoint discrimination on a given platform?

Mr. COX. Yes. I'm a big fan of transparency. I think the devil always is in the details. The question is, you know, How steep is the compliance burden, and is it, you know, such that it will, you know, expose platforms to, you know, liability that they will need to structure around and try to protect themselves from, which could have some unintended consequences for the availability to all of us of user-generated content. But, the ambition of using the law and all the other tools that we have at our disposal to encourage and get, where transparency is a good one, you can imagine, for example, that if the rules of the road were much more explicit and un-

derstandable in every case, and if, when decisions were made, for example, to cancel somebody's account or to take down material, that the decision was directly tied to, you know, specific provisions in those rules that people could understand, and the decision-making was publicly available so we could all learn from it, we would all be, you know, more likely to abide by those terms of conduct online, because we would understand them. I hold we would be better off, it would be achieving its aims more successfully, and then, hopefully in the process, the Internet would be a little more civil.

Senator THUNE. And you stated in your testimony that the PACT Act's content moderation transparency component, and as I quote from your testimony, "unquestionably constructive and consistent with Section 230 in its ultimate aims," end quote. What content moderation transparency requirements do you think are most important to apply to Internet platforms? And how do transparency requirements benefit consumers?

Mr. COX. Well, just further to the points I was making, you know, consumers sometimes operate in the dark. And when take-down decisions are made and then people get up in arms about it and talk about it on the Internet—we can all see what people are saying—you know, a lot of the complaint is, "What the hell are they doing? What are they thinking? Their terms of service say X, but they did Y," and so on. So, the more information that is provided so that people can understand decisionmaking, the better off we're all going to be.

In my written testimony, I've provided some extensive commentary on very specific aspects of the PACT Act that bear on this question. I think that, you know, ultimately what you need to focus on and be concerned with is, How is this going to operate in the real world? Is it actually doable? Is it workable? Are, you know, the data-collection requirements or the reporting requirements going to be such that they might actually interfere with the realtime aspect of Internet communications who don't wish to do that, because that's an essential feature of how the Internet operates and what its great benefits are? You know, is it going to put platforms in a position where the liability that we thought we protected them from for using user-generated content just, you know, evaporates? You know, we don't want to be in that position, either, because we know what they would do. Many of them will feel the need to jettison user-generated content, or to vastly restrict it.

So, those are the guardrails that I think we want to observe. The objectives are equally clear.

I just don't see what's in it for platforms to be opaque. It's not in their interest to do so. And I think that many of them have been making big steps in this regard. I also think it's important that more resources be devoted to this. The bigger platform, the more resources we can expect to be devoted to this.

Senator THUNE. On that——

Mr. COX. And I would——

Senator THUNE. On that——

Mr. COX. Yes, go ahead.

Senator THUNE. On that point, I would turn to Ms. Banker, because—you made this point, Representative Cox, but, Ms. Banker,

you noted that IA's member companies have been working to enhance content moderation transparency with their users. Today is there a minimum transparent requirement platforms have to meet? And it seems like, as Representative Cox noted, it would be in their interest not to be opaque, to be as transparent as possible. What's happening in that space right now?

Ms. BANKER. Thank you, Senator.

IA member companies are voluntarily enhancing their transparency around content moderation activities. The—Internet companies actually have a long history of being transparent. Early transparency reports generally focused on topics like the disclosure of user information to law enforcement. But, in recent years, the companies have been working steadily to expand that into content moderation topics, as well. There is not a minimum standard. And, you know, we appreciate the focus of the PACT Act on this area, but do want to make sure that, should new requirements be put in place, that they're requirements that all of IA members would be able to fulfill. And we represent both large and small companies and a multitude of business models that are other than social media, which tends to be the focus of most of this discussion.

Senator THUNE. Yes. Thanks.

Senator Schatz.

Senator SCHATZ. Thank you, Mr. Chairman.

I'm going to start with Professor Sylvain. You went very quickly on a very important point, and I want you to flesh it out a little bit.

Can you describe exactly what happens when a company invokes Section 230 and tries to win on summary judgment, avoid discovery, avoid a lawsuit? Regardless of how the statute, whether it be in civil rights or the extension of credit or education or housing, that statute would normally carry the day, or at least get a plaintiff a day in court. But, with Section 230, they just invoke it, and there's—and it's the end of the conversation. Could you flesh that out a little bit?

Mr. SYLVAIN. Thank you for the question, Senator Schatz.

And just to be clear, the way—the moment it's invoked in litigation is at the motion to dismiss, generally, not in a summary judgment. At summary judgment, there will be—you know, they will have—discovery will have—some discovery will have happened already. It's invoked at the motion to dismiss, before any discovery. And what the courts are doing, as you say, is, they're not reviewing the substantive statute under which any plaintiff is alleging some harm. What they're doing is evaluating whether the defendant is—meets the qualifications of the safe harbor, or the—as people call it, the immunity under Section 230——

Senator SCHATZ. In other words, whether they're online.

Mr. SYLVAIN. Whether—that's right—whether they're interacted computer service, which is, basically, whether they're online.

And then, the further question, which is a point that Jeff—Professor Kosseff started with, is, they evaluate—you know, moving away from the old case law on this, evaluate whether they're being treated as a publisher or distributor in—under the claims—under the legal theory brought by plaintiffs. And if they are, that effectively shuts down the litigation. And the things that count as pub-

lishing are pretty expansive, so I invoked the advertising case—the Ad Manager case, because it underscores how broad this claim is. It includes the sorts of things that social media companies do when they distribute content. It might also include advertising. Indeed, it does include advertising. Right? So—and I think——

Senator SCHATZ. But, would it matter—I'm sorry to interrupt, but would it matter whether the platform was intentionally violating a—say, a civil rights statute or a housing statute or a banking statute? Or would that Section 230 immunity sort of obviate the inquiry into the question of whether it was sort of like them hatching a plan or whether or not they were just simply allowing it to happen as a result of their systems and algorithms?

Mr. SYLVAIN. That's a really good question. Could a company that intentionally wanted to perpetuate some harm under public law do so, and be comfortable doing so because they would be treated as a publisher in—a distributor under a claim, and would never—we'd never find out what their intent is? I think that would be—I mean, I would be curious to see what that case looks like—I think it would be hard to imagine, if they weren't also content—contributing content in that circumstance, if they weren't also creating and developing content in that circumstance. But, I suppose you might envision such a thing. And the closest I can think of is the Jones case, wherein the Sixth Circuit reviewed a plaintiff's argument—this young woman who alleged that she was being defamed by a site that elicited comments that were abusive about young women. And, you know, the—one of the things the Sixth Circuit is entertaining is whether another standard, not the material contribution standard, would be relevant. But, in any case, that comes close to the scenario you've just mapped out. The Section 230 defense was victorious in that case.

Senator SCHATZ. In other words, we'll probably never find out what was in the minds of the people who were the—whether it's de facto discrimination or it was intentional. We would just not—not know, because you wouldn't get past the motion to dismiss.

I have a question for all of the panelists. Everybody understands, who's participating in this hearing, that a series of rulings have established that platforms are not obligated to remove or address illegal content, a 1997 decision and then a 2010 decision. And so, the question for the panel—I'll start with Mr. Sylvain, followed by Ms. Banker, Mr. Cox, and Mr.—and Professor Kosseff. Do you think the platform should be required to remove content that has been found to be illegal?

Mr. Sylvain, yes or no?

Mr. SYLVAIN. Yes.

Senator SCHATZ. Ms. Banker?

Ms. BANKER. I think that, much like in the PACT Act, you've made provisions for that. I think that's a fruitful area of inquiry, but we'd want to make sure that there are safeguards——

Senator SCHATZ. What does that mean? I'm sorry. It's a yes-or-no question. Should illegal content—we're talking about not supposing that something is illegal. A court determines that this is illegal content, and you represent the Internet Association here. Should there be a statutory requirement that illegal content—court-determined illegal content be removed from websites?

Ms. BANKER. Our companies have no interest in hosting known illegal content, and most of them would remove it voluntarily. But, I think, if there is a requirement, we'd just want to be sure that there is sufficient guardrails to make sure that the court engaged in a thorough review. Unfortunately, we've also seen why—the variety of instances where these types of mechanisms have been subject to abuse.

Senator SCHATZ. Where a court has determined that content is illegal, and somehow we need additional guardrails? I mean, it's not like that happens all the time, right?

Ms. BANKER. No, but it—frequently, plaintiffs do go into court seeking that type of ruling, with an eye to having content taken down. Unfortunately, not all of those cases, you know, are brought in good faith. We are lucky. Some states have tools, like anti-SLAPP Act provisions, that can be used to make sure that individuals who are exercising the right to comment on matters of public interest are able to do so. But, not in every case is a defendant able to show up and defend themselves in court. So, we just want to make sure that, you know, to the extent we are covering things like defamatory content, that there are safeguards.

Senator SCHATZ. Congressman Cox.

Mr. COX. Yes, I think that a well-crafted statute could do a lot of good here. I see no reason that court order and certainly final judgments requiring the takedown of content already adjudged to be defamatory, for example, couldn't be enforced. If the law were to provide clear standards for platforms, telling them how they should handle defamation judgments, just to use the paradigm situation, especially in cases in which the platform hasn't been sued, such as is the case in the California Supreme Court with Hassell against Bird—I think that was 2016—and the platform isn't the party to the litigation, and so it's essentially succeeding in keeping these disputes out of its hair without fear of liability. This is consistent with the aims of Section 230——

Senator SCHATZ. Thank you.

Mr. COX.—injured party would receive justice. That's a positive outcome for everybody except the fellow who broke the law and lost in court. So, it's exactly the way Section 230 should work.

Senator SCHATZ. Professor Kosseff.

Mr. KOSSEFF. Yes, absolutely, if something has been adjudicated to be illegal, I think it should be taken down, just with the caveat that there have been cases of court orders being falsified because there are many platforms that already honor the court order. So, we want to just make sure we have a provision to take care of that.

And I would also add that, in addition to defamation judgments, we might want to look at, also, family court judgments, because defamation can be a very expensive process to go through, and, in some of the most harmful content—stalking, harassment—people are not going through the full defamation process. So, I think we'd want to look at that, as well.

Senator SCHATZ. Thank you very much.

Senator THUNE. Thank you, Senator Schatz.

Senator Wicker.

The CHAIRMAN. Thank you very much.

Very, very good panel. Very helpful.

Critics of the Communications Decency Act argue that the words "otherwise objectionable" allow social media companies to remove content they simply dislike or disagree with, without facing liability. So, that raises the question how social media platforms inform their users about what constitutes "otherwise objectionable content."

As I mentioned in my opening statement, the content that is available to be removed already includes "obscene, lewd, lascivious, filthy, excessively violent, harassing," those words. So, the question is, Would it be helpful if we removed the somewhat ambiguous term "otherwise objectionable"?

So, Mr. Cox, let me start with the very beginning. What does "otherwise objectionable" mean to you, as an author? And what was the intent behind the inclusion of that term in the original statute?

Mr. COX. Of course, what the statute says is, you know, most important, and that's the standard to which people need to conform their content, that's what vendors need to interpret, and so on. I think what I intended, what Ron intended when originally we wrote this, and what Congress intended when it considered the legislation and voted for it, were all consistent with how we would want it to work. And that is that this string of words that's followed by "otherwise objectionable," you know, has to be read as a whole. It's a well-established rule of statutory interpretation that when general words follow specific words in a statutory enumeration, the general words are construed to embrace only things similar in nature. It's a legal rule known as "ejusdem generis," which is Latin for "of the same kind." It's a rule of long standing that's been reaffirmed by the U.S. Supreme Court in the 21st century. So, the words "otherwise objectionable" have to be understood with reference to the list of specific things that precedes them. It's not an open-ended grant of immunity for editing content for any unrelated reason a website can think of.

But, it's necessary not to be too stingy in, you know, setting out in the statute, you know, what is covered, because there are a lot of really bad things we'd like to see taken down from the Internet, some of them maybe not invented yet, that would be, you know, just as objectionable and just as, you know, categorically fitting as what we've listed specifically. So, we don't want to deprive websites the opportunity, you know, to keep their sites clean and civil and so on. But, that's the rubric. You know, it's—it doesn't take you far afield into anything that I personally idiosyncratically as a website don't like. That clearly is not what the statute says. And one hopes——

The CHAIRMAN. What—Mr. Cox, what about it—political speech? Does "otherwise objectionable content" include political speech?

Mr. COX. Well, you know, political speech sounds like a broad category, but it's easy enough to imagine that somebody decides to take something down because they disagree with it. You know, "You say that taxes should be higher, I say they should be lower. I don't like what you said, and I'm taking it down." You know, that's not a good reason to invoke Section 230. That's not what that Good Samaritan piece is all about. And I think that you would have to find some other reason to be protected for doing that. And

there are plenty of other good reasons that a website can say, "We don't want to put your political point of view up here."

The CHAIRMAN. OK.

Mr. COX. But, not Section 230.

The CHAIRMAN. Let me quickly move to Ms. Banker.

What type of content do your member companies consider to be "otherwise objectionable" that—where the content is not already covered by the preceding terms of the statute, which I just quoted in my question to Representative Cox?

Ms. BANKER. Thank you, Senator.

There's a wide range of types of content that are covered by our member companies' policies, and they are often dictated by what the business model is of the particular company. So, in addition to social media members, we also have companies that have travel information, you know, dating sites, job sites. And what's appropriate for one of those platforms may not be appropriate for one of the others. So, it's really important for our member companies that they have broad protections to be able to engage in the type of content moderation that helps users have a positive experience on their services and also builds trust and confidence in their services.

One example is one I used in my testimony, which is spam, which is something that courts have applied "otherwise objectionable" to. And I think, you know, obviously, it has a broad impact on the usability and enjoyment that people have around online services.

The CHAIRMAN. Why don't we just add "spam" to the definitions, and take out "otherwise objectionable"?

Ms. BANKER. I think you can certainly do that. I think that that would be narrow, and there are many things that we cannot necessarily predict today. Many of our member companies, for example, have taken positions against hate speech on their platforms, and a narrow definition of "otherwise objectionable" could very well, you know, inhibit their ability to feel like that's something that they can do.

The CHAIRMAN. Thank you.

Thank you, Mr. Chairman.

Senator THUNE. Thank you, Senator Wicker.

In my day, "spam" was a meat product, so we'll have to define that, probably, in the amendment, too.

Next up is Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR, U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much.

And thank you, to you, Senator Thune and Senator Schatz, for not only holding this hearing, but really walking into this and trying to take this on. I truly appreciate it. I think we all know that Section 230 has played an important role in allowing the Internet economy to develop from its humble beginnings, but now these aren't just scrappy startups anymore. They are, at times, trillion-dollar companies and some of the largest companies in our global economy, and raises many questions of how Section 230 is not working, and changes that must be made. And I have some other

views on the antitrust side that I'll save for Judiciary, but this is our focus today.

So, I've done a lot of work in the area of misinformation in elections with the Honest Ads Act. And, Mr. Sylvain, one of the most heartbreaking unpaid ads that went out and was targeted on African-American pages in the 2016 election was a picture of an African-American woman, and it said, "Why wait in line in this election? You can text your vote for Hillary at 83456," or pick some numbers. To me, it was a crime, but it spread all over the Internet and was targeted at their pages.

In your testimony, Mr. Sylvain, you note that Section 230 has helped perpetuate discrimination and racism against members of historically marginalized groups. Do you believe that proposals to reform it should consider the spread of election-related disinformation and how it is targeted at certain groups?

Mr. SYLVAIN. Thank you for the question, Senator Klobuchar.

Yes, I do. The trick is, of course, trying to sort out how to do that. One would be allowing the Federal Elections Commission, presumably, to entertain enforcement actions consistent with what the PACT Act sets out. But, you might imagine civil rights groups also being able to initiate actions if this is the kind of electioneering that is against the law. Section 230 does pose an obstacle for that.

One question that I'd like to ask in this context is whether the law does, indeed, engender a sense of obligation—of civic obligation. And in a circumstance, the one you've just described, I suppose it might, after the fact; but, in the first instance, it obviously didn't. And so, there are a variety of circumstances under which we can envision a statute being written in ways that do encourage intermediaries to intervene before the damage is done. And the conventional way we do that is—as Senator Schatz, earlier on, said—is articulated in law. Online intermediaries are immune from that obligation, because they——

Senator KLOBUCHAR. Right.

Mr. SYLVAIN.—might act, under the doctrine, as a publisher or a distributor.

Senator KLOBUCHAR. And, you know, the other way I think about it is just with this pandemic and the misinformation going out. Last month, one study found that 38 percent of Americans believe that the coronavirus outbreak has been overblown. And, just last week, Facebook had to suspend a group for spreading disinformation about wearing masks. And I just think, again, it's just a visceral reaction that I have, and I think many lawmakers should have, regardless of party, when these platforms are used in that way.

Let me turn to you, Mr. Cox.

Thank you, Mr. Sylvain.

I noticed—I listened carefully in your testimony, and you talked about transparency, and you talked about—Congressman, about how you wrote the law to consider the future, which I truly appreciate. And if you knew then what you know now about the importance of large platforms in our election, the oversized importance, and how they've been exploited by foreign adversaries, which has been validated by Trump intelligence officials, to influence and un-

dermine our democracy, would you have written any protections for our democratic system into Section 230?

Mr. COX. Well, I think that watching the case law develop over the last quarter century has been quite an eye opener. And when all of you retire from Congress and have a chance to watch what the courts do with your handiwork, it will, in many cases, make you proud, and, in other cases, disappoint you. It's—so, some of what has gone in interpretively with Section 230 has shocked me. And I would say most of the courts have read the statute and gotten it right.

I think one of the most important parts of the statute is the definition in (f)(3) that covers the situation in which a platform, itself, is actually involved in the illegal content or activity or conduct. This is not something that, you know, came to our attention in later years, after we wrote the law. We thought about this at the time, and we wanted to make sure that if the website was actually the problem, that the website could be prosecuted criminally and it could be sued civily.

Senator KLOBUCHAR. Mr.——

Mr. COX. So, it's taken away. So, what I would do, Senator Klobuchar, if I were, you know, back then in 1996, and knowing what I know now in the 21st century, is probably write a 30-page essay around section—subsection (f)(3).

Senator KLOBUCHAR. OK. But, we don't have—the 30-page essay isn't going to stop the Internet mess that has been created when it comes to these political ads. And our problem is that we don't have any requirements in place right now for disclaimers or disclosures, not just for the campaign ads. And some of the platforms have either stopped running political ads or they have done it themselves. But, it is a complete mishmash, what is going on. And we have a situation where they don't have to put disclaimers, disclosures. I'm not just talking about campaign ads. I'm talking about issue ads. And billions and billions of dollars have migrated from TV, radio, and newspaper that have those requirements over to online platforms that don't. And that is our issue. And we—Senator McCain did the bill with me. Senator Graham is now a cosponsor of the bill. And it is separate and apart from 230, but it would help with this type of illegal activity. And that's what—why I bring it up to you now.

Mr. COX. ——

Senator KLOBUCHAR. OK. All right.

Thank you.

Senator THUNE. Thank you, Senator Klobuchar.

Senator FISCHER. Senator Fischer? Senator Fischer, you want to turn your mic on?

STATEMENT OF HON. DEB FISCHER,
U.S. SENATOR FROM NEBRASKA

Senator FISCHER. Am I on?

Senator THUNE. There you go. Yes.

Senator FISCHER. OK. Thank you.

Congressman Cox, in your testimony, you described the First Circuit's dismissal of BackPage.com as an outlier. And you noted that the court did not reach the sensible decision on the law in the first

place. Yet, we continue to hear concerns from law enforcement that Section 230 limits their ability to undertake enforcement actions in cases dealing with illegal content online. Clearly, we're dealing with daylight between these takes on the law, here. So, I know that Senator Schatz touched on this in his question and also Senator Klobuchar. In your answer to her, you addressed some of the concerns on Section 230, the effects on hindering case discovery in prosecution. I'd like to ask you how we can best support enforcement actions to keep illegal content off of the Internet.

Senator THUNE. Senator Fischer, who was that directed to?

Senator FISCHER. Congressman Cox.

Senator THUNE. Chris, are you there?

Mr. COX. Thank you, Senator. Yes, I'm here. And excellent question. And it's the right focus. Because, as is noted, it was the original intent of this law to be completely consistent with law enforcement aims and also with civil redress. So, what we want to do is, again, punish the guilty and protect the innocent.

The law gives us tools that aim in the right direction. First of all, Federal criminal law is completely unaffected by Section 230. And State law that's consistent with Section 230, likewise. What we'd like to do, on the law enforcement side, I think, is get the states more deeply involved. And one way to do that and not lose the benefits of a uniform national policy that Section 230 represents would be to extend the limited opportunities that we have in law right now for State attorneys general to be deputized by the Department of Justice to enforce Federal law and/or State laws that are, you know, run in parallel with the Federal law when Federal law is also violated. And the PACT Act, you know, gets, to a certain extent, some of this going. I think there's even more that we could do, and I've mentioned, you know, specifically how in my written testimony.

On the civil side, just a quick word about how the law ought to operate. I think it is vitally important that there be objective standards that judges could apply at the pleading stage, where you have to assume that all the allegations in the complaint are true, and determine whether or not a website, you know, has to, you know, enter upon a long litigation involving, you know, civil discovery and so on. I don't think that every case should go into discovery "just because." And so, the nice thing about Section 230 is, it has an objective test: Were you a content creator, or did you contribute or develop it? I'd like to keep that in anything that we do, because otherwise the sheer volume of third-party information on the Internet would mean that every single piece of content now, you know, is a potential 3- to 7-year litigation.

Senator FISCHER. Right. Thank you.

Mr. Kosseff, would you also comment on the tension that we see with Section 230 and with law enforcement?

Mr. KOSSEFF. Yes. So, I fully agree with Congressman Cox about providing state—the states with the ability to enforce both Federal law as well as State laws that parallel Federal law. The only concern might be if there were 50 different significant variations of State laws applying to Internet platforms, which we see in other areas of the law, like data security. I also think that the use of the existing Federal criminal exception is very important. For example,

Backpage having been shot down a few days before FOSTA was signed into law because of that Federal criminal exception. But, I fully agree that there should be some balance to allow some State enforcement.

Senator FISCHER. You know, we're seeing case law that's been developed that's protecting a wide range of platforms for many different types of claims there. How do you address that, then? What do we need to do?

Mr. KOSSEFF. Just to clarify, civil claims? Yes. I mean, obviously, because of the increase in the complexity of the Internet, there is a wider variety of claims that go far beyond defamation. And I think, as Congressman Cox said, the key is, Did the platform contribute, in whole or in part, to that content? And if it did, then then Section 230 is not going to apply.

Senator FISCHER. OK. Thank you.

Thank you, Mr. Chairman.

Senator THUNE. Thank you, Senator Fischer.

Next up, Senator Blumenthal.

STATEMENT OF HON. RICHARD BLUMENTHAL, U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thanks very much, Mr. Chairman.

Senator THUNE. And in person. In person.

Senator BLUMENTHAL. In person.

I really want to thank you and Senator Schatz for having this hearing and for your efforts to take a broad look at the continued viability of Section 230 and the need for reform. And I think if there's a message to the industry here is, it is: the need for reform is now. There's a broad consensus that Section 230, as it presently exists, no longer affords sufficient protection to the public, to consumers, to victims and survivors of abuse, and others who deserve greater protection.

Earlier this month, the Judiciary Committee overwhelmingly approved the EARN IT Act. In fact, it—the vote was unanimous. It's a reform to Section 230 specifically crafted to fight online child sexual exploitation. I have worked with Senator Graham on it, to go back to Senator Schatz's comment at the beginning. We actually engaged in bipartisan legislating on the EARN IT Act to modify it in committee with a manager's package that met just about all of the potential real objections, including the impact on encryption.

While working hand-in-hand with survivors on the EARN IT Act, I was struck by the predicament that they face in combating sexual abuse of children. And I really want their voices to be heard today. And so, I'm going to ask that we make a part of the record a statement from Nicole, whose mother—whose daughter was a victim of sexual abuse, and she said—and I'm quoting, if there's no objection, Mr. Chairman——

Senator THUNE. Without objection.

[The information referred to follows:]

Statement by

Nicole, Mother of a Child Whose Sexually Abusive Images Were Circulated Online

Senate Judiciary Committee

March 11, 2020

Good morning, Mr. Chairman, Ranking Member Feinstein and esteemed members of the Senate Judiciary Committee.

My name is Nicole, and I want to thank you for the opportunity to be here today to represent myself, my family and all child sexual abuse material (CSAM) survivors who need a voice.

I am here today to give you a firsthand view of how CSAM affects the children who are depicted in the images and their families. So many of the children affected cannot have a voice – maybe they are still being abused, or they are afraid of being recognized, maybe they fear retaliation or maybe – hopefully- they are just trying to press forward to live the life they deserve to have. It is a privilege to speak on behalf of these amazing survivors and their families to talk about how the EARN IT Act could change the path for them.

WHAT HAPPENED TO ME AND MY FAMILY

It was a typical Wednesday morning until 9:24 AM when I received a phone call from a Detective in another city. He asked to see me right away and said he could be at my home in an hour. I was confused as to why a detective would want to see me.

It was the longest hour of my life waiting for him to arrive and in that moment life as I knew it was over. He said that sexual-abuse images of my child had been found in the Netherlands and had been forwarded to the National Center for Missing & Exploited Children (NCMEC) in Alexandria, Virginia. Analysts at NCMEC were able to trace the images to the city where the Detective worked. He in turn was able to identify the person who had produced them: my child's biological father.

I learned that he had started taking the abusive images when our child was 5 years old and continued doing so for more than 7 years. He had also been sharing these images on the Internet, and at that point, this series of images was the most highly traded in the world. They were everywhere - the dark web, social media sites such as Facebook and Instagram, and Wikipedia. Everywhere one could look for this filth the images were found.

That same day my child's abuser was arrested, and exactly two years to the day later he was sentenced to 60 years, eight months to Life in state court for the abuse he perpetuated against my child. He then accepted a plea for 30 years in Federal prison and currently resides there until he is sent back to our state prison system in 2035. After he was criminally prosecuted, I successfully terminated his parental rights and changed my child's identity.

Through this experience, I learned about a world of online child sexual exploitation I never knew existed. NCMEC's peer support group, Team HOPE, helped me through my ordeal. Our local and federal law enforcement supported us, encouraged us and most importantly fought for my child to get justice.

CONCERNS/FEARS

Even after the legal process was behind us, we endured a very difficult time. My child, who was a teenager when this horrible crime was revealed, received therapy and counselling. But it never occurred to me that the repercussions from the abusive images of my child circulating would be harder to overcome than the physical and emotional trauma my child had endured.

I was very naïve on that Wednesday morning because I felt relief there were images so there was proof of what he had done, and he could not lie his way out of whatever charges he was facing. I learned that NCMEC has seen my child in 168,474 files found across thousands of offenders collections of CSAM submitted to them by law enforcement. Even today, a decade later, these images are still being traded and found in new cases, and I know this because the Department of Justice sends out a notification letter each time these photos are distributed. We still receive a ton of notifications.

When I learned the images were still being circulated after his arrest, I was astounded that there were very few safeguards in place to prevent the distribution and redistribution of CSAM. I was frustrated that even with all the technological advancements there was no way to completely remove this type of material from the internet. Even more frustrating was the fact that the criminals always seemed to be one step ahead of the good guys who were working to eradicate CSAM. I learned that once these images are uploaded and shared, they will continue to be distributed for many more years. Once we learned how widespread the images were and how many more times these images could be redistributed across the internet, I became afraid. Afraid someone would recognize my child, afraid these images would haunt my child into adulthood but mostly I was afraid of the fact that they would never, ever stop being circulated.

Ten years later the advancements are even more impressive but there is still work to be done. The technology should be expanded to identify live streaming as well as grooming behaviors in order to proactively stop and prevent abuse. Companies should do more to prevent CSAM from being redistributed over and over again on their services. They should also include non-abusive images of a child who has been identified as the subject of CSAM. In our case the photos that held the evidence that led to my child's identification were all non-abusive images. Alternately, we have found images of the abuse material that have been cropped to redact the abuse but show my child's face in its entirety.

Every single company who hosts user uploaded content is responsible for identifying, removing and reporting all CSAM, known and unknown. Companies who do not do this are complicit in the abuse and need to be held accountable just like an individual person would be. Under the Terms of Service of most providers they own the content uploaded by users and should be fully responsible for it once received.

Statement by

Nicole, Mother of a Child Whose Sexually Abusive Images Were Circulated Online

Senate Judiciary Committee

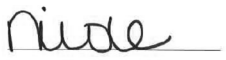
June 30, 2020

Dear Mr. Chairman, Ranking Member Feinstein and esteemed members of the Senate Judiciary Committee:

I have become aware of the changes being proposed in the manger's package to the EARN IT Act in the months since I testified before you. I want to express my support of the markup with the manager's package and no other amendments before you vote on this Bill. I am in favor of these changes because I firmly believe the EARN IT Act is something that makes the rights and safety of CSAM survivors a priority. Every time a CSAM image is shared the child is revictimized and every single company who hosts user uploaded content is responsible for detecting, removing and reporting all child sexual abuse material, whether it has been previously identified or is new CSAM. Companies who do not do this are complicit in the abuse and need to be held accountable just like an individual person would be. Survivors need to have all their remedies under the law – including federal and state law – so they can decide when, where, and how to seek justice against everyone who has been part of their abuse.

This Bill is about the safety of kids and there is nothing more important than protecting them.

Thank you for your time and I am deeply appreciative of your efforts to protect children like my own.



Nicole

Senator BLUMENTHAL. Thank you. "Child sexual abuse is one of the worst things that anyone can endure. The production, distribution, and possession of CSAM make it so the abuse is relived every time the material is viewed or shared." She fought, for years, to rid the Internet of those abusive images, and many of them are still there. Her child was abused for 7 years.

So, we know that these images can spread like wildfire, in milliseconds, each time victimizing the survivor again. The images of Nicole's daughter were shared 168,474 times by thousands of predators on social media, each time a new trauma, decade after decade.

I appreciate the Chairman and the Ranking Member's work, but I'm very concerned about the burden that's placed on the victims and survivors like Nicole. If we take Nicole's nightmare, the images of sexual abuse of Nicole's child were shared on Facebook. Under the PACT Act, to achieve any kind of remedy against Facebook, Nicole would have to undertake a number of steps. First, she'd have to go to court and obtain an order declaring the images illegal, an unnecessary step, or it should be, when it's plainly clear her child was sexually abused. And then Nicole would have to submit to Facebook a sworn statement containing the court order and, quote, "information reasonably sufficient to permit Facebook to locate the content." Again, the burden on the victim. She would have to find all the abuse images on Facebook, herself, a tremendous burden. And only then, if Facebook failed to act, could Nicole go to court to guarantee that the image is taken down. Again, the burden on the victim.

The PACT Act does not provide any incentive for Facebook to police its own platform. Instead, it puts the obligation on Nicole. It is, unfortunately, cumbersome, costly, time-consuming, and it would offer Nicole no real relief in ending her daughter's nightmare. And, in the meantime, those images would spread as she had to undertake the burden and the obstacle of seeking a court order. Going to Facebook, going back to court, and then seeking additional litigation to guarantee that the image is taken down, the images would be spreading.

Under the EARN IT Act, Nicole could go straight to court, stop the images, and, if Facebook has failed victims, a court can require real changes in behavior and impose actual remedies, with real teeth, that provide incentives for Facebook to do better. And what applies to Facebook here would apply to all of the platforms. They can no longer be regarded simply as a independent and immune means of conveying a message without any responsibility, any accountability. To quote Nicole, "The EARN Act is about the safety of kids, and there is nothing more important than protecting them." I encourage my colleagues to listen to her words.

Thank you.

Senator THUNE. Thank you, Senator Blumenthal.

Senator Moran.

STATEMENT OF HON. JERRY MORAN,
U.S. SENATOR FROM KANSAS

Senator MORAN. Chairman Thune, Ranking Member Schatz, thank you very much for this hearing.

Thank you, for our witnesses, for joining us.

This is a question intended for all of our witnesses. Increased automation in the form of artificial intelligence to improve content moderation and other functions used by technology companies, along with many other sectors, many critics and policymakers, including me from time to time, have called for certain degrees of algorithmic transparency to ensure increased consumer insight in how automated decisionmaking is informed, but there is also an inherent question of preserving the proprietary value of innovative algorithms that fuel the competitive drive among industry actors.

How should we, as policymakers, consider improving algorithmic transparency for consumers without upsetting the economic competitiveness and innovation pursued by the industry?

It's odd asking questions to no one I can see.

Senator THUNE. Who wants to take the first stab at that one?

Mr. COX. Well, I'd like to go second——

[Laughter.]

Mr. COX.—but, since nobody is speaking up, I will put my oar in the water.

You know, this is the future. Increasingly, we're going to see artificial intelligence taking over, not just social media decisionmaking about how they promote material and so on, but really all of the management of data across the Internet, in all manner of contexts. And it raises questions, in jurisprudence, about liability and responsibility, because if people can, in the future, say, "The computer did it, and none of us knew that that was going to happen, we had no actual knowledge," then it would become, you know, the greatest loophole ever invented into law.

I think we need to not be distracted by the complexity—and there is a good deal of it—of code-writing and the way that algorithms are deployed, and the way that artificial intelligence increasingly is being deployed, and stick with enduring principles of the law, as best we can.

I would take this all the way to a principle of writing statutes and drafting to try to avoid all the jargon, to the extent you can, because, when you put that jargon in the statute, one of the unintended consequences is that compliance is now going to adhere to whatever tech you put in the statute, and it prevents them from advancing and coming up with the next best thing. So, stick with general principles.

And what's the general principle here? It is that human beings write the code. So, ultimately, I think the simple answer is, imagine a room full of 50 people that did the same thing that the algorithm did, and what would you do? What would the legal result be in that case? And I think that that will lead us to the right answer.

Senator MORAN. Anyone want to take the second position that Congressman Cox wanted to have?

Mr. SYLVAIN. If Representative Cox doesn't mind, I'll take the second position. I'm grateful that he went first.

First, I may be wrong on—I'll be happy to be corrected—I thought there was a Algorithmic Accountability Act in consideration on the Hill. So, I take Senator Moran's question to be addressed to that, as well.

There are a couple of ways to—I—so, I agree that it has to be part of the way we think about intermediaries. My testimony is addressed to automated decisionmaking systems, and I'm particularly interested in the question of how we render them accountable. And one of the ways we might do that is requiring some kind of—what people who write in this, including Andrew Selbst, who's written about this a lot, is an algorithmic impact statement evocative of the sort of things we envision in other areas of law. So, that's one way of making this work.

But, for what it's worth, it also speaks to the question of what we are rendering accountable. For those people who write and study in this area, there is a question of the extent to which any given algorithm or automated decisionmaking is explainable and understandable to most people. And generally they're not. Most of us—Representative Cox, right?—are not code-writers. But, on the other hand, there might be a way to convey it in ways that are meaningful to the public, and an impact statement might be in that vein.

Senator MORAN. Thank you.

Mr. KOSSEFF. I'm happy to go next, just to echo what was said before. And what I would just add is that behind algorithms, there are policies that are informing them, and I think the first principle is to make policies as transparent as possible. And we're seeing some progress on that. I would point to Facebook, I believe, last year, releasing a far more detailed list of its community standards, not only with just principles, but with some fairly specific examples of what is allowable and what's not allowable. And I think that's really at least a first step in any transparency, is understanding what policies are driving this.

Senator MORAN. Thank you.

Senator THUNE. Thank you, Senator Moran.

Senator UDALL. Remotely. Senator Udall.

STATEMENT OF HON. TOM UDALL,
U.S. SENATOR FROM NEW MEXICO

Senator UDALL. Yes, you got me?

Senator THUNE. There you go. Got you.

Senator UDALL. Great. Thank you.

Chairman Thune, thank you so much, you and Ranking Member Schatz, for calling this hearing and focusing on this really important issue.

President Trump's recent executive order on preventing online censorship directs various Federal agencies to protect against online censorship, under the claims that, quote, "online platforms are engaging in selective censorship that is harming our national discourse," end quote.

Just yesterday, the NTIA filed a petition for rulemaking with the FCC, asking the agency to develop rules to moderate online content under Section 230. As Commissioner Rosenworcel has said, the FCC shouldn't take this bait.

This question is to all of you on the panel. Can you speak to the legal grounds of the President's executive order? And what recommendations would you make to the Department of Justice and

the FCC for how they should evaluate this information to maintain the constitutional protections under the First Amendment?

Mr. SYLVAIN. I guess everyone wants to go second. I'll take a shot, here.

I am deeply skeptical about the nature of the way in which the FCC could proceed, although, you know, I can envision it happening, but the FCC would have to do a lot of work to reverse the ways in which it has, basically, discounted its obligations or authority under law to interpret and apply Section 230. This is to say nothing of whether there is a—there are First Amendment concerns with regards to the SEC regulating speech.

And I want to go further and say, in my opinion, the focus on user speech is a distraction from actually the way in which the constitutional protections for intermediaries works. Ultimately, they are the ones to resolve what their interests are with regard to what they allow online, even consistent with 230(c)(2). And that's my own view.

I also think the focus on speech, as though these platforms are speech platforms, as such, is distracting. Consistent with my point in the opening, these are commercial entities that traffic in user data. And they have the prerogative to do so, but there are few constraints on what they can or can't do.

Senator UDALL. Thank you.

Others, jump in, please.

Mr. COX. Well, I'll take the opportunity to go second, which I was, you know, always hoping for.

[Laughter.]

Mr. COX. Because now that Professor Sylvain has laid the groundwork, it's much easier for me.

A couple of things. When originally we wrote what—became Section 230, when Ron and I introduced a freestanding bill, it was called the Internet Freedom and Family Empowerment Act, and mostly what became Section 230. It contained a provision that explicitly denied the FCC authority in the area of regulating the content of speech. And what I said on the floor at the time is, we don't want to turn the FCC into the Federal Computer Commission.

I would like to see the FTC be more active in this area. I'd like to see the FTC, you know, holding platforms to their promises. You know, when they advertise that they're neutral platforms, by all means hold them to it. I think the error in the executive order that President Trump issued, in analysis—the error in analysis—is in thinking that there's something about Section 230 that requires all websites, including the Republican National Committee's website, the DNC website, to be politically neutral. That's just wrong. The law can't—shouldn't—require that, and it makes no sense to do so.

But, when platforms adopt business models, when they make promises to consumers, when they have rules of the road of content moderation, when they have terms of service, those are, you know, essentially, advertisements and contractual promises that can be enforced. That's why we have an FTC. It's why we have State consumer protection laws. Let's enforce them. Let's use——

Ms. BANKER. I would just add to both of those comments and say I think it's incredibly important, when we think of how—availability of Section 230 or it going away completely, what is the law

going to do then? And I think there have been a number of cases brought against providers, in the last several years in particular, over content removals. And in those cases, many times what the users whose content was removed are arguing is that their First Amendment rights were violated. And we have repeatedly—you know, without any involvement in Section 230—and we've repeatedly seen courts say, "No, these private companies are not—they're not State actors, so they cannot violate First Amendment rights."

So, I think the focus on Section 230 to address the problem that the EO aims to address is a little bit misplaced, because I don't think it's necessarily a Section 230 problem, I think it's more—if you consider it a problem, it's probably a First Amendment problem.

Senator UDALL. Professor Kosseff?

Mr. KOSSEFF. Yes, I would just echo what's been said, and I would also just add—and this isn't—there have been a number of proposals—this isn't specific to the executive order, but the one challenge in all of this—and there have been a lot of discussion about conditioning Section 230 protections on certain editorial behaviors. And that runs into the additional First Amendment consideration of unconstitutional conditions. We've seen, in other areas of the law, where, if you withhold a government benefit, that—in exchange for a specific type of speech—that can run into constitutional problems. It's kind of a unique situation, so it requires more exploration, but I think that's at least one thing to look out for.

Senator UDALL. Thank you.

You know, this executive order came out after the President's many public complaints that various online outlets are not favorable to him. And Twitter, notably, flagged one post for inciting violence when he tweeted, quote, "When the looting starts, the shooting starts," end quote.

So, I think I'll end there, Mr. Chairman.

Thank you so much, to all the panelists.

Senator THUNE. Thank you, Senator Udall.

Senator Gardner.

STATEMENT OF HON. CORY GARDNER,
U.S. SENATOR FROM COLORADO

Senator GARDNER. Thank you, Mr. Chairman.

Thank you, to the witnesses, for appearing today.

According to Pew Research, approximately 5 percent of Americans used a social media platform in 2005. Five percent, the first year they started collecting that data. As of last year, that number had grown to at least 72 percent. Globally, social media and Internet adoption numbers continue to rise. Most of the world's biggest social media platforms—things like YouTube, Facebook, Twitter, WhatsApp, and more—are companies founded right here in the United States. This growth in activities spurred by American innovation that I hope will be a boon, and should be a boon, to free speech, democratic values, and greater understanding of differences around the world.

You certainly see that reflected in the mission statements of these companies today. YouTube says, "Our mission is to give everyone a voice." Facebook says their platform exists to, "give people

the power to build communities and bring the world closer together." Twitter wants to, "give everyone the power to create and share ideas and information instantly, without barriers." And WhatsApp says their goal is to "let people communicate anywhere in the world, without barriers." And yet, the most recent Freedom on the Net report from Freedom House concluded that Internet freedom declined yet again for the ninth year in a row, even as social media adoption continues to rise.

So, Congress and the world should ask itself, Why is that? For one, government censorship is alive and well around the world. In countries with repressive regimes, questions of intermediary liability always involve that repressive regime at the table. Each of these major social media platforms I've mentioned—YouTube, Facebook, Twitter, and WhatsApp—are banned and behind the great firewall in China. Their missions of empowering people and sharing information, without barriers, don't exactly align with the Chinese Community Party or the Chinese Community Party platform.

Even in allied countries like Germany, international organizations like Human Rights Watch have lambasted local content moderation laws as unaccountable over-broad censorship rather than sensible public empowerment. The United States should be pushing back on this global tide of government regulation, censorship, and blocking.

There is no question. Any social media platform who claims to be a forum for all and then engages in politically motivated content moderation is not a platform living up to its stated mission. And those platforms must be more transparent. But, should Congress involve itself in enforcing so-called neutral content moderation? What does "neutral content moderation" even look like?

Congressman Cox, we're lucky to have you here today testifying as one of the two major authors of Section 230, someone who can give us that clarity about what Congress really intended when it drafted this statute, insights obviously critical to policymakers as we consider next steps and whether or not this statute needs amending at all.

On August 4, 1995, going into the wayback machine, you took to the House floor and declared, "Our amendment will do two basic things. First, it will protect computer Good Samaritans from taking on liabilities such as occurred in the Prodigy case. Second, it will establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet, that we do not wish to have a Federal Computer Commission with an army of bureaucrats regulating the Internet, because, frankly, the Internet has grown up to be what it is without that kind of help from the government."

So, Congressman Cox, do you think Congress has paid enough attention to the second tenet of what you said in 1995 was a fundamental aspect of Section 230? Or do you believe Congress should still view Section 230 as what helped establish the policy of the U.S., that we do not wish to have content regulation by the Federal Government?

I'll turn it over to you, and then I've got another question for you.

Mr. COX. Well—and that's great history. I have a twofold answer to your question. The first is, I do think that Congress has paid attention and observed that policy as the policy of the United States in practice, because it has not, to date, imposed, you know, stifling regulation on the Internet. But, I will say that the public discussion right now around these issues is paying little heed to that same norm. And so, as we reevaluate where we're headed next, I think the question's very much on the table.

You noted the Freedom House annual reports on how we're doing across the planet with social media. And what we see in their report is not just that China and Russia and Iran and Saudi Arabia, all known cases, are using social media as a means of social control, reading people's, you know, communications and punishing them, you know, if they're online, and so on. And then you have got a system of social credit, you know if you don't agree, you can't go to school, you can't get an apartment or get in an airplane, leave the country, what have you. The point——

You know, our model—different, but—this is a problem in 38 countries covered in their last report——

Senator GARDNER. Yes. And I have a——

Mr. COX.—around the world.

Senator GARDNER. I'm out of time. I want to follow it up with a quick question, here.

As the world continues to consider aggressive Internet regulation and Goulburn at Freedom continues to weigh in, it's more important than ever that we are communicating American ideals about fundamental human rights and First Amendment protected free speech abroad. How should Congress better enlist the support of technology companies in that mission? What more can Congress and American tech companies be doing to make the Internet a truly free, or a freer, and safer place for all?

Mr. COX. Well, you know, I'll—go—I'm sorry, go ahead.

Senator GARDNER. No, no, that's it. Go ahead.

Mr. COX. You know, the challenge that our global companies face in the 38 countries highlighted by Freedom House, for example, where they're trying to control the Internet and use it as a means of control are very significant, because the companies themselves obviously can't conduct foreign policy; they need the assistance of the U.S. Government. But, you know, one of the questions that has been widely debated this past year is whether, when we negotiate our trade agreements, we should be pushing for this principle, that we want to protect user-generated content, because, you know, the ability that we all have to post our things on public forums is derivative of Section 230 in, you know, protecting the platform from liability for that. And liability will be a reason that they won't host our speech, and we won't have that avenue if we take Section 230 protections away.

So, should we try and put this in our trade agreements? I believe we should. But, you know, people that are concerned about, you know, some of the issues that we have here in the United States, which they don't have in other countries because they don't have any freedom of speech, in many cases, or it's, you know, deeply suppressed because of the government's exercise of its regulatory control over social media and the internet itself. So, they've taken

those concerns that we have here in America, which I think we can work out and use that as reasons, and not put—the broad principles into our trade agreement.

So I think number one, use our trade leverage and use our diplomacy, and put the Federal Government's, you know, foreign policy-making as the wind at our back so that our—platforms, you know, can——

Senator GARDNER. Thanks.

Mr. COX.—and so that the Internet can be visible, globally, and people can have access to more information around the world.

Senator GARDNER. Thanks.

Senator THUNE. Thank you, Senator Gardner.

Next up is Senator Peters.

STATEMENT OF HON. GARY PETERS,
U.S. SENATOR FROM MICHIGAN

Senator PETERS. Well, thank you, Mr. Chairman, for this hearing.

And, to each of the witnesses, appreciate your testimony today.

I—Mr. Sylvain, the first question I have is for you. African Americans make up a little less than 13 percent of the United States population, but accounted for over 38 percent of U.S.-focused ads purchased by the Russian Internet Research Agency, and almost half of the user links. The social media accounts generally built a following by first posing as being African-American-operated, and by paying for ads that social media companies then distributed largely to African—or to African-American users. And near election day, the accounts urged African Americans to, quote, "boycott the election."

So, my question to you, sir, is—African Americans make up 14 percent of the population in Michigan. What recommendation do you have to prevent these targeted ads from disenfranchising voters? And what kind of oversight mechanisms could Congress possibly implement?

Mr. SYLVAIN. This is one issue that I find extremely difficult to wrestle with and think about. I do think that Twitter and Facebook have put a good step forward insofar as they have asserted that disinformation in regards to elections is the sort of thing that they were going to try to be proactive about.

You're asking whether or not Congress can do more. In my—and consistent with my testimony, I wonder whether there is a mechanism that Congress can undertake, apart from what Section 230 reform, as set out in the PACT Act, would do.

Let me just speak about the PACT Act. I talked, a moment ago, about the possibility for civil enforcement. I—you know, I—again, I'm not an election expert, but my sense is that the sort as content that you're describing is fully inconsistent with public law in the context of elections, and so there might be some opportunity for intervention by an agency in that setting.

But, the—you know, the other way I think about this—and this is an indirect question—in a way—indirect way of answering your question—I think that the big social media companies, the ones through which a lot of this content has been distributed, and also through WhatsApp, by the way, which is even more difficult to

track, is pursuant to an interest in maximizing user engagement, and in spite of whatever the content is. And sometimes there's a kind of disregard for the content until an alarm bell is rung. And I think part of the reason that the content—that misleading information about elections could flow to African Americans, whomever, in election years, is because, in the first instance, it's a—it's drawing attention, apart from whether it's disinformation. So, the arguments I've made is that you—that companies might be more alert to their social obligation if they are already attuned to the obligation to attend to law. So, this is the indirect answer. The salutary effect of imposing obligations on companies to attend to law is to attend to things like election tampering through social media.

Senator PETERS. Well, thank you.

Congressman Cox, you noted that the ideal way to screen wanted information from unwanted information is not for the government to regulate that flow, but rather for each individual user to have, basically, the greatest possible control over what they actually receive. Right now, as you know, private companies have significant control over screening what an individual sees or does not see through their algorithms.

Question for you is, What are your thoughts on providing, perhaps, individual users with algorithm options that they can take greater control over what is presented to them?

Mr. COX. Well, I think that sounds like a wonderful idea. I mean, the more tools that we have as users of the Internet, all of us, to customize the content that we receive, the better that's going to be, from our perspective, for sure. You know, whether or not those tools will be, you know, freely available, whether they'll be expensive and we'll have to buy them, I don't know, but I'm all for it. I hope that, increasingly, such tools are available. As you know, you know, going back to the original law, that hope is expressed as one of the reasons that we adopt a law is to make sure that we have, you know, continued technological development, that regulation doesn't stifle it, and so on.

But, just last, I would say that, insofar as, you know, parsing who should be in charge of deciding, you know, what's on the Internet, you know, only if we're talking about material that is legally acceptable in the first place, you know, does it then become the primary responsibility of the Internet user to determine whether he, she, or it wants that, you know, on their computer and in their premises. But, if it's illegal material per se, then that's the government's business, and it should be the platform's business to be concerned with that, as well. And so, we want to get as much of that off of those—the servers in the first place.

Senator PETERS. Great, thank you.

Mr. SYLVAIN. Senator Peters, do you mind if I jump in one last—for one last point?

Senator PETERS. Yes, please.

Mr. SYLVAIN. I know your time's up.

Just real quickly. I mean, as Representative Cox was talking, it struck me that there is another specific tool that we haven't yet raised or discussed but that, I admit, is more controversial, and that is looking at targeted advertising. And maybe there's a way to think about restrictions in targeted advertising in the context of

politics and elections. This—it is, in many ways, probably a—it's a constitutionally thorny question, but it's—because we already have rules against electioneering that are addressed to speech, I—you know, for example, what you can do outside of a voting station—I wonder whether that's another possibility.

Senator PETERS. Great.

Senator THUNE. Thank you, Senator Peters.

Senator Cruz.

STATEMENT OF HON. TED CRUZ,
U.S. SENATOR FROM TEXAS

Senator CRUZ. Thank you, Mr. Chairman.

Thank you, to each of the witnesses, for being here today on this important topic.

Representative Cox, let me start with you. Thank you for your long service and for your friendship. You and I have had interesting and substantive conversations on this specific topic of Section 230 and speech online. And I appreciate your expertise.

When you were part of drafting Section 230, it was 1996. It was a long time ago. And, as you stated in your testimony, the Internet looked dramatically different than it does today. At the time Section 230 was written, there were roughly 20 million American adults who had access to the Internet, which compares now to more than 7-and-a-half billion globally, which is roughly 375 times as many people have access to the Internet as they did when Section 230 was drafted.

In 1996, the principal means of access was dial-up, something, as you talk to young people today, that they don't even know what dial-up is. But, the speeds were so mind-numbingly slow that it would take 10 minutes to download a single low-quality song, and anywhere from 3 to 5 days to download a single low-quality movie. The world has changed dramatically, and the money and power that has been concentrated in Big Tech is altogether different. In 1996, the Internet was still a nascent technology, and a technology that was very much being incubated from the ground up.

Representative Cox, when you helped draft 230, was Google a company? Was Facebook a company? Was Twitter a company?

Mr. COX. No, not at all.

Senator CRUZ. So, none of them existed. There was no player that had the dominant monopoly position that we see, particularly at Google, in terms of controlling search, controlling access to videos, and being in a position to potentially manipulate search outcomes and silence views with which they disagree.

In your opinion, should we be concerned about Big Tech censorship? Is it a problem that should trouble, not just Congress, but the American people?

Mr. COX. Well, thank you, Senator. And there's a lot to unpack, here.

You know, first, you're looking back to 1996, and even 1995, which was older still, and that's when Ron and I started on this. The concerns that we had at the time, I think are even more powerful in today's 21st-century context, because what we were concerned about was this essential distinction between the new technology, the Internet, and all that had preceded it, that government

had found a way to regulate newspapers, television, and radio, where there was one group of content creation—the TV station, the radio station, the newspaper editorial staff—and then, you know, millions of passive recipients. With the Internet, you had millions—it was millions even back then, in the 1990s—of content creators who would then, you know, instantaneously broadcast to the whole world. What we could see, if the platforms were given the legal responsibility to monitor all of that content constantly and take legal responsibility for it, well then you couldn't have the Internet, you couldn't have realtime communication and—among, you know, millions of people around the planet. So that today the fact that it is billions, and not millions, makes the problem all the more stark. And if you impose that liability on the platforms——

Senator CRUZ. So, Representative Cox, if I could ask if you could focus your answer on the question I asked, which is, Should the American people be troubled that a handful of Silicon Valley billionaires have monopoly power to silence speech they disagree with and amplify views that they agree with?

Mr. COX. Well, so I don't want to miss the point of your question, so may I answer this question within the framework of Section 230, or do you want me——

Senator CRUZ. I'm just asking if you agree it's a problem, not—I think the solution is complicated, but I'm just trying to start with, Do you agree this is a real problem?

Mr. COX. Yes, so I think it—first of all, if a platform is holding itself out as neutral, and, in fact, is not, and, in order to accomplish its objective of not being neutral, it is covering up the fact that it is, you know, doing things behind the scenes that it disclaims, then I think you have, you know, a violation of a lot of existing laws, and that it is absolutely something that we should be troubled about. Whether or not that's exactly what's happening—you know, this is something of a hypothetical question—but, whether or not that's exactly happening obviously is the fulcrum of what we do about it.

Senator CRUZ. So, Representative Cox, my time is expiring, here, but I want to make an observation. One document that I would encourage you to take a look at is a document that Google drafted and that was a major focus of a subcommittee hearing that I chaired some time ago. And the document is entitled "The Good Censor." Now, this is a Google document they wrote, in which they described how the old view of the Internet was what they described as laissez-faire free speech. It was the model you were talking about, of lots of content producers, let them speak, let's have a free-speech forum. And then they described the new model of Big Tech, which is what they called "European-style censorship," active censorship. You know, you talked about companies purporting to be neutral. According to Google's document, they listed four companies that had moved from laissez-faire free speech to European-style censorship. Those four companies were Google, YouTube, which Google owns, Facebook, and Twitter. By their own terms, they're not being neutral. They are actively censoring and, given the monopoly power they have over free speech, I view that as the single greatest threat to our democratic process that we have today.

Thank you.

Senator THUNE. All right. Thank you, Senator Cruz.

Senator Lee is up next. And I'm going to hand off to Senator Schatz and go vote.

So, Senator Lee, recognized.

STATEMENT OF HON. MIKE LEE,
U.S. SENATOR FROM UTAH

Senator LEE. The United States light-touch regulatory approach to the Internet has been good. It's been good for the world economy, and for the American economy, in particular. It's produced, for us, an incredible success story of free speech and of innovation that really no other country in the world can boast.

Section 230 is, I think, a significant part of that success. But, the Internet, like all other things, is not free of bad actors, bad actors who may be to try to use this resource for harmful and damaging, in some cases deceitful, purposes. But, in order to find the solution to those evils, we need to understand the problem.

So, let me start by asking Mr. Kosseff and Ms. Banker, Are today's Internet problems—that is, political bias, illicit content, et cetera—caused by Section 230 immunity?

Mr. KOSSEFF. I guess I'll go first. That's an excellent question. And I think it's hard, because I think the success of the Internet and the prevalence of the Internet has certainly amplified problems. I wouldn't say it's necessarily directly——

Senator LEE. Not the cause.

Mr. KOSSEFF.—Section 230.

Senator LEE. Right.

Mr. KOSSEFF. But, Section 230 being responsible for the success of the Internet in the United States, clearly the Internet has more of an impact, but I wouldn't say that it's Section 230 itself that's causing the—there are a number of different factors.

Senator LEE. Ms. Banker, what do you think? Do you agree?

Ms. BANKER. Thank you. I'd actually say something perhaps a little bit different, which is, I think that, in terms of the types of harms we see on the Internet today and the voluntary measures that the Internet companies engage in to try and address those harms, we're actually enabled by Section 230. It is the protection that companies receive under the law for their voluntary efforts to try and enforce rules around illegality or just objectionable content that, you know, has, I think, put us in a better place today than we would have been without Section 230.

Senator LEE. All right. That's good to know. Thank you.

I want to talk a little bit about viewpoint discrimination among Big Tech, particularly among the big social media platforms. It is concerning. It's concerning on a number of levels, that you see what has become, I think, increasingly blatant viewpoint discrimination going on within these platforms. Now, to be sure, these platforms are not instrumentalities of the government. They're not government property. And yet, there is something concerning; in part, because, from my vantage point, centralization of power leads to centralization of government power. It makes it easier for government to take control of these levers, and it can cause other problems.

Now, if I've been informed correctly, Donald Trump, Jr., the President's son, has, as of today, been suspended from Twitter. Why? Well, I'm told because he posted something containing content posted yesterday by a number of medical doctors who were speaking their mind as to what they view as the appropriate course of treatment for COVID–19. Now, I strongly suspect there might be an ideological angle, here, or it might have something to do with the fact that he's the President's son. Either way, this is concerning; in part, because these kinds of things tend to influence public policy and public debate.

I don't think I've ever seen that kind of action taken by a social media platform when preferring one view on how to treat strep infections over another, or one view about how to treat cancer over another. So, that is concerning here.

Nonetheless, I'm not so sure that Section 230 reform, or repeal, is necessarily the answer we're looking for. I think we need to find an answer to these questions. And I hope that that answer can be found within the market, itself, and not through government. But, I don't think 230 is the way to go.

Now, Mr. Cox, in your 1995 floor speech, which Senator Gardner alluded to earlier on why Congress needed to adopt Section 230, you noted the relationship between adoption of Section 230, on the one hand, and avoidance of Federal regulation of the Internet. You argued that Section 230, quote, "will establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet, and that we don't want to have a Federal Computer Commission with any—with an army of bureaucrats regulating the Internet." So, I think you're on to something here, but I'd like to ask you. Since your 1995 speech in Congress, has Section 230 helped the United States avoid government regulation of the Internet, and of Internet content, and allowed for Americans to have access to many viewpoints at the click of a button?

Mr. COX. Umm, well the answer to that is yes, I think so. And, you know, with the benefit of hindsight, looking back over a quarter century of experience, not just in the United States but around the world, we can see the other model. It exists now in technicolor. So, take a look at the great firewall in China, take a look at the way that Russian media is organized, and take a look at Iran and Saudi Arabia, and then go down the list of the 38 countries that have been flagged by Freedom House as using social media for population control, and you can see, you know, the other model in its extreme. I don't know that, you know, the United States, with its, you know, democracy and, you know, for the most part, benign government looking after, you know, people's rights and so on, would have ended up there in any case, but if you're looking for the extreme dystopian alternative to the system that we did choose, it exists now today in the world. So——

Senator SCHATZ [presiding]. Senator, if I—we'd like to move on. We're over time. We have a number of members to speak.

Let's move on to Senator Baldwin.

STATEMENT OF HON. TAMMY BALDWIN,
U.S. SENATOR FROM WISCONSIN

Senator BALDWIN. Thank you.

I really want to appreciate Chairman Thune and Ranking Member Schatz for having this hearing today.

You know, it's important, and it's a thoughtful conversation, for the most part. And it goes without saying that the Internet of today looks very different from what existed when Section 230 was first authored and adopted in 1996. But, as we've already heard from many of our witnesses, that is, at least in part, because of Section 20—230. So, I think it makes a lot of sense for us to take a hard look at this law in light of all of the changes we've seen. But, I also think we have to approach any potential reforms with thoughtfulness and humility.

Section 230 allows online platforms to moderate the third-party content that they host. Its Good Samaritan provision arguably encourages platforms to do so proactively. But, there has been a great deal of criticism of companies that have fallen short in their content moderation, whether by failing to promptly remove content that violates their own policies, lacking clarity and transparency about those policies and their enforcement, or appearing to apply those policies in a biased manner.

There are a number of proposals, including the measure introduced by the Subcommittee Chair and Ranking Member, that would take steps to incentivize, encourage, or require better content moderation practices, including more transparency and due-process protections for those whose content is removed. And I think there's a lot of value in having platforms improve their content moderation efforts. But, I'm also concerned that a more proscriptive requirement or set of requirements could lead companies fearing litigation to overcompensate and push more content off their platforms.

So, I'd like to get the whole panel's views. Is there an approach by which we can incentivize active, clear, and consistent content moderation without the negative consequences of less-open platforms and fewer new entrants into the Internet ecosystem?

And let me begin with Professor Kosseff.

Mr. KOSSEFF. Thanks so much for the question.

And I think you really hit the nail on the head, in terms of what the challenge is, here. Because, I mean, the balance that Section 230 has at least attempted to strike is to give the platforms breathing room to develop their own content moderation and both not become liable for everything that's on their system because they're doing some moderation, and also not become liable if they're aware of something and make a judgment call to leave it up. Because content moderation at scale is incredibly difficult.

So, I think that moving more toward transparency, rather than being proscriptive and saying, "You must do this," because it's hard to get a one-size-fits-all approach for every platform, but giving the public a much better—much better insight into how the platforms are working, I think that's a very positive first step, and I think some of the platforms are really taking steps by themselves to move in that direction.

Senator BALDWIN. Mr. Sylvain? Professor?

Mr. SYLVAIN. Yes, I actually agree with a lot of what Professor Kosseff just said. I think—and you hit the nail on the head, that the question of incentives matters, and we might have—this is a circumstance where, on the one hand, we do want to encourage moderation, but, the other hand, we may not want to chill too much speech. And so, on that principle, I think we can all agree.

The only difficult, for me, is that the—as embodied in current law, that's just not good enough with regards to content that is harmful to historically disadvantaged groups. And so, I do think we need more than, you know, standardized conceptions of how to do moderation. I think the PACT Act sets out a really interesting transparency map and a—process for takedown. But, I do think we need more. And that's where law comes in.

You know, there's a—I'm not the first person to observe that—you know, that law engenders public regarding, to take a language that Senator Schatz used at the outside, kind of public-interest, public-regarding norms. Law does that. And so, how do we formalize that, as a matter of course, rather than rely on companies' moderation standards? That's the tough question, and I think I err on the side of seeing more law play a role, here.

Senator BALDWIN. Congressman Cox? Good to see you, by the way.

Mr. COX. Well, one of—yes, thanks—one of the reasons that I am so enthusiastic about seeing more enforcement around content moderation policies, you know, getting the FTC involved, getting a consumer protection enforcement involved, is that I think Section 230 already provides plenty of space for companies to do things voluntarily; and the maddening thing is when they don't, anyway. So, when someone brings an egregious case of law violation to a platform, if the platform says, "You know, we have no legal responsibility to do anything here," that's—that, to me, you know, is an outcome, you know, we should dearly wish to avoid. And so, how about looking to see whether that platform ever promised that that kind of illegal stuff was not going to be allowed? And if they said, "We take these sorts of things down," and don't, then I think you've got, you know, plenty of grounds for enforcement.

But, more than, you know, a Section 230 all by itself is necessary, here. There's got to be, you know, some backbone provided to the very sensible steps that I think common sense suggests that, you know, platforms should be taking. And most do, to their credit. But, the cases where they don't, you know, immediately reach our attention. And when I was in Congress, as you all still are, you know, the nice thing was, I'd pick up a newspaper, and if there's an outrage, and say, "Ought to be law," then, you know, we'd go fix it.

We have laws that I think are even being used that we can apply to this situation, because there are promises being made, and they extend even sometimes to political neutrality and so on, as Senator Cruz was mentioning. When those promises are violated, the courts have held that they can be enforced.

Senator SCHATZ. Senator Blackburn.

STATEMENT OF HON. MARSHA BLACKBURN,
U.S. SENATOR FROM TENNESSEE

Senator BLACKBURN. Thank you so much.

And, Mr. Cox, welcome over to the Senate side.

Mr. COX. Yes.

Senator BLACKBURN. It is good to see you.

You and I have talked about Section 230 for years. And, as you were working on it in the mid-'90s, of course, I was in Tennessee and chairing the Tennessee Film Entertainment Music Commission and watching closely what you all were doing here. And, of course, through this time, the Internet has grown.

I think that in 2018, when we did FOSTA and SESTA, and I was in the House and chairing Coms and Tech, we were pretty much looking at the fact that there were reforms that were needed, there were things that needed to be done, updates that needed to be given. And our concern is, you have some of our social media companies that have grown to the point that they function, in the words of Facebook's founder, more like a government. And they ought not to be making those decisions as to prioritization of content or availability of content on their sites.

So, let me ask you this. And raise your hands. As you look at post-230 cases, are there any of those that any of you panelists would say have been wrongly decided?

Mr. COX. Well, I will jump in, if I may. Oh. Raise my hand.

Senator BLACKBURN. OK. Go ahead.

Mr. COX. Yes, in my written testimony, I laid out, in some detail, how I think the First Circuit got it wrong in the BackPage litigation. The First Circuit, at least at the District Court level, subsequently in 2018 rectified its mistake and interpreted Section 230 correctly, I think, as against the pleadings that it was looking at in that case.

Senator BLACKBURN. All right.

Professor Kosseff?

Mr. KOSSEFF. So, Congressman Cox took my answer that I think that case actually pointed more toward the discovery problem that we've discussed earlier, the lack of the ability to get discovery in extraordinary cases on whether the platform contributed to the content.

Senator BLACKBURN. OK.

And let me ask—and I'll start with you, Professor Kosseff, since your mic is open—as we look at the statute—of course, Congressman Cox helped to author that statute—do you believe that it is time, and that it is actually necessary, for us to revisit and to reform this statute based on concerns that are in the marketplace now?

Mr. KOSSEFF. I think revisit, in terms of gathering better facts—as I said earlier, having a commission that gathers facts about, for example, what's possible with content moderation at such a large scale. I don't think we're at the point of being able to reform, because we have so many competing viewpoints about what platforms should be doing on top of what we could require them to do because of the First Amendment and other requirements. So, I think Section 230 is so important that we really have a duty to always look

at how it's working, but I think right now we really need to be gathering more facts.

Senator BLACKBURN. OK.

Congressman Cox?

Mr. COX. Yes, I agree with that. I think the real challenge is figuring out what's doable in the real world. When I look at some of the legislation that's been introduced, such as the EARN IT Act, you know, which contains, you know, 16 separate categories of new, you know, regulatory requirements that are going to apply to websites, you know, these websites are all very different. They're not all Facebook. They're not even in that business. They're not all social media companies. And there are big differences between, you know, Twitter and Google, even at the Big Tech level. So, you know, what's doable, and what's going to, you know, on the other hand, you know, put at risk the availability of the user-generated content that we all rely on? And I think that, you know, we need to be careful of doing things like the EARN IT Act does, which is to say, well, we're——

Senator BLACKBURN. OK. Let me ask you——

Mr. COX.—we're just not going to create a commission such as Professor Kosseff suggests, but we're going to give that commission legal authority that Congress won't even have an opportunity to check on, and it won't be something to Administrative Procedure Act public input or anything else. It'll just happen. So, I think we need a little more humility than that.

Senator BLACKBURN. Should it be left with the FTC?

Mr. COX. Well, I think the FTC has a role. But, as I said, I think the FTC can do a lot of enforcement around false advertising, around, you know, the consumer abuses that have been identified. But, I think, you know, there are a lot of different laws and law enforcement levels, not just the Federal Government, but States, as well, can be our allies here.

Senator BLACKBURN. OK. My time has expired, so I will yield back, but I'm going to send to each of you a question on what you think we should do so that we're protecting free speech online and we are still making certain that the social media outlets do not practice censorship or prioritization.

Thank you so much.

Yield back.

Senator SCHATZ. Senator Tester.

STATEMENT OF HON. JON TESTER, U.S. SENATOR FROM MONTANA

Senator TESTER. Yes, I want to start by thanking you, Senator Schatz and Senator Thune, for your good work on this issue.

And I want to express my appreciation to everybody's who's testified here during this hearing.

I want to shift the conversation a little bit, at least I don't think it has been here. I had to get off for about a half hour. But, when a broadcast station, whether it be TV or radio, hears false or misleading advertising, they can be held accountable by the FCC or a court of law. However, I don't see the same consequences for Internet platforms.

So, I have two questions. Number one, Is this right? Is this the way it should be? Is this the way it was intended when you wrote it up, Congressman Cox? And, number two, How did we get here? How did we get to this point?

And I'll start with you. I'd like to have everybody address it, but I'll start with you, Congressman Cox.

Mr. COX. Yes. Thank you, Senator.

The challenge that this poses is only matched by its importance. I think it's—important for us to get it right, because this goes to fundamental operation of our democracy.

The difference—there are big differences between the radio and TV and newspaper paradigm, and the Internet. And that's what creates the disparity, because the essential functioning of the Internet is based on not just, you know, 10 or 50 or even 100 advertisers coming to the TV station, saying, "Here's our ad. You know, check it out and put it on the air." Instead, it's millions of people, or billions of people, around the world, because it's a planetary potential user base. And the question is, Is it reasonable for the law to presume that the platform has the opportunity to review all of this material? And, if they were to have the obligation to review all of it, is it even conceivable that that could be done in realtime? And, if not, are we willing to say that——

Senator TESTER. Yes.

Mr. COX.—the regulation can do away with that essential aspect of the Internet, which is realtime communication——

Senator TESTER. The point is, though, Congressman, on paid advertising—in paid advertising, do you believe that they have an obligation to review that, just as TV and radio and newspaper do?

Mr. COX. Yes, well, and this may be an area where the existing rules could reasonably apply, because it is reasonable to expect that a company, a platform, has the opportunity to review its paid advertising before putting it up. You know, that may or may not be the case, depending on the business model. But, if that's the way it actually operates—it's why, you know, the real-world aspects of this are so important—then I think the way at least 230 was conceived, you're not risking an unreasonable burden on the platform that would cause it to dump user-generated content all together.

Senator TESTER. Mr. Sylvain, could you respond to that, also? I'd love to get your perspective as to, when it comes to paid advertising, should the same rules apply to the Internet platforms as does the TV, radio, and newspaper?

Mr. SYLVAIN. Thank you for the question, Senator Tester.

Senator TESTER. I'm talking about from an information standpoint——

Mr. SYLVAIN. Yes.

Senator TESTER.—being misleading.

Mr. SYLVAIN. Yes. I do think so. And I'd like to start by getting to your second question first: How did we get here? The business model on which a lot of the most prominent intermediaries rely really is focused on maximizing or optimizing user engagement. And often that is at the expense of veracity. In some cases, that's OK. But, there are certain circumstances where lies and misleading and information and disinformation are costly for the oper-

ation of democracy. And our electoral system is one of them. So, we have a—the prevailing business model accelerates the distribution of provocative content, because it's consistent with the interest of engaging users. And often this is the kind of content that might misdirect people with regards to our political system.

So, that's how I think we've gotten here. And so, I'm more alarmed—and I think many members have already expressed in this hearing—about disinformation online, so much so that I do think this is an urgent opportunity to align electoral law with what we see in other communications platforms.

Senator TESTER. Thank you.

—you've only got about 20 seconds. Could you respond, to the best of your ability, quickly?

Ms. BANKER. Yes, I'll be quick.

I think the platforms understand that, with regard to advertising and its importance, that they have stricter policies and heightened enforcement. But, I just—I want to add a caution, too, about the tremendous benefit that the new ad ecosystem has had for small businesses, because it has, essentially, lowered costs so that businesses that previously could not have afforded to advertise are now able to. And, as a former restaurant owner, I can tell you that, for small businesses that are cash-strapped, the ability to, like, really target advertising to a key demographic, and be able to do that quickly and easily, is a huge benefit. So, we'd want to make sure that, if any changes are made, that, you know, the costs don't end up again making advertising out of the reach for critical small businesses.

Senator TESTER. Thank you all.

And thank you, Chairman Schatz.

STAFFER. Senator Rosen, you're next.

STATEMENT OF HON. JACKY ROSEN,
U.S. SENATOR FROM NEVADA

Senator ROSEN. Thank you so much. Thank you, Chairman Shune, Ranking Member—Thune—Ranking Member Schatz.

Thank you, to all the witnesses, for being here today, and your work in this area.

I'd like to speak a little bit about the bias in algorithms, and particularly in hate speech. Because one of the issues commonly raised regarding content moderation across multiple platforms is the presence of bias in artificial intelligence systems that are used to analyze the content. Decisions made through AI systems, including for content moderation, run the risk of further marginalizing and censoring groups that already face disproportionate prejudice and discrimination, both online and offline.

As a former computer programmer and systems analyst who began my career when the field was even more dominated by men than it is today, I find this particularly troubling, because we've had previous hearings, where the witnesses—they've discussed the harms that algorithmic and AI systems potentially pose, including those from biased training data, algorithms, other system flaws that reproduce historical and existing social inequities. We see this when firms have tried to automate their hiring through machine

learning, but then find that it merely perpetuates existing biases toward women.

But, what I want to do, besides sexism, is to talk about another alarming issue that's happening today. Another challenging—another challenge that we're facing is hate speech. And so, when we use algorithms, and we deal specifically with the growing prevalence of anti-Semitism and the hate speech that's perpetuated online, this is bypassing content moderation, if such moderation exists on these sites at all.

Last year, we saw the deadliest attack in the Jewish community in American history, when 11 people were killed at the Tree of Life Synagogue in Pittsburgh. Then, perhaps unsurprisingly, the shooter was linked to numerous anti-Semitic postings on fringe social network sites. This one, in particular, called Gab.

So, for all the panelists, knowing that our online platforms are running into issues with content moderation specifically as regards to algorithms and AI systems, how should mainstream social networks interact with these fringe sites to stop the spread of manifestos, letters, other hateful writings?

So, Congressman Cox, perhaps you can start; go then to Ms. Banker, Professor Sylvain, and then Professor Kosseff, please.

Mr. COX. Yes. So, there is so much work to be done in this area, because, despite the best efforts of even the most well-motivated social media platforms, you know, we see examples where the algorithms don't work, sometimes the algorithms even serve up, you know, opportunities for bad people to, you know, get together. So, we've got to be constantly vigilant.

We've talked about the legal incentives that exist. We've also talked about what more law enforcement could do in cases where platforms are actually interfering with the right outcomes. I think the most troubling challenge for writing law in this area is, you know, what about the great middle ground, where people are not—that have the platforms, they're not bad actors, they're trying to do the right thing, but it just doesn't amount to enough? And you suggested something that I think can be a way forward, and that is that there be collaboration among all the people with good hearts here to advance best practices and so on.

The term "best practices" has been bandied about in some ways that are constructive, and others not. For example, in connection with the EARN IT app. But, I think the development of best practices in some ways, along the lines that Professor Kosseff has suggested, and then, you know, pushing those out to smaller websites, and so on, could be an absolutely constructive way to help.

Senator ROSEN. Appreciate that.

Ms. Banker, can you speak to the process with, perhaps, algorithm and AI systems that we have to moderate content with?

Ms. BANKER. Absolutely. Algorithms are obviously incredibly important today. You know, they help us from everything to finding the fastest route to get to work to things like content moderation.

The specific area you were asking about, you know, hate speech, is an area where—you know, algorithms alone are not going to be able to get us there. There's a critical role for human reviewers, and many of our companies, you know, use that, or rely on that,

you know, primarily for these things where context is incredibly important.

And I would also note that, in terms of industry collaboration, we've seen that work well in other contexts. You know, in 2006, you know, Internet companies came together to form a—kind of a coalition working together to share technology, know-how, and information to address the issue of child sexual abuse material. And, more recently, they've done something similar to address terrorism.

So, I think there's precedent for that, and it's certainly an issue that the companies care about a great deal.

Senator ROSEN. Thank you.

Professor Sylvain, quickly. I know my time's expired. Perhaps I'll leave you with the last word. Anything to add on AI and algorithms?

Mr. SYLVAIN. Well, I would have loved for Professor Kosseff to jump in. I'll just say, quickly, that——

Senator ROSEN. Well, if Ranking Member Schatz——

Mr. SYLVAIN.—align this point——

Senator ROSEN.—would let him, we'll be glad to, yes.

Mr. SYLVAIN. Just one quick point, and that is, I would associate—I don't have anything to add with—on—based on what everyone else has said. I will say that the question of what is objectionably offensive, I very much appreciated Representative Cox statutory interpretation lesson earlier. You know, we think about what is within the subjective decisionmaking prerogatives of intermediaries. And I think this is squarely in it, for what it's worth.

Senator ROSEN. We'll give you, then, the last word, Professor Kosseff.

Mr. KOSSEFF. Thanks so much.

I agree with everything that's been said. I would just also add that there have been some significant failures, and we can't ignore that. But, Section 230 does provide the flexibility for experimentation with the best and most innovative procedures. We have to look at whether that's working. But, that is kind of the underpinning of Section 230.

Senator ROSEN. Thank you. I appreciate y'all being here today.

Senator THUNE [presiding]. Thank you, Senator Rosen.

We're about ready to wind up, here, guys, so thanks for your indulgence and your patience, and even for, while I was off voting, since we have so many people who are appearing virtually, remotely, including members of the Committee, sometimes it's hard to cover the gaps when we've got votes going on, so I understand staff had to step in. So, thank you for very ably picking up the slack here.

I'm going to ask just, if I might, perhaps one question, sort of close it out, and then we'll wrap things up.

But, Representative Cox, Jeff Kosseff notes, in his prepared testimony, that CDA 230 has sometimes shielded platforms from plaintiffs who've suffered serious harms, and that, while Section 230 does not block a plaintiff from suing the person who created the harmful content, there are a number of reasons why that might be impractical, including the inability to track the person down or fear of retaliation.

And one very recent example is the case of *Force v. Facebook*. And, in that case, the Estate of Taylor Force, who was killed in a Hamas terrorist attack in Tel Aviv, alleged that Facebook's algorithm provided the Hamas terrorist group with the means to find each other and to share content celebrating terrorist attacks. The Federal Court shielded Facebook from liability, on the basis of Section 230.

So, the question is, How should Congress deal with this particular scenario, where a plaintiff, who has unquestionably been harmed, is unable to seek justice?

Representative Cox.

Mr. COX. Yes, thank you.

You know, that was a very tough case that you mentioned. It's an excellent example of the kinds of novel questions that the courts are going to face increasingly as technology, and, in particular, artificial intelligence, is going to play a greater role, not just in social media, but the—you know, their overall exploitation of data on the Internet.

This case came out of the Second Circuit, which I noted in my written testimony has followed the national trend of applying the Ninth Circuit's rule in Roommates.com, which I credit for, you know, really taking us a great step forward in the development of the common law under Section 230. I think Roommates.com got it right, particularly when the Ninth Circuit considered that case en banc. In that case, the court held that a website was not entitled to protection from liability under Section 230 because it contributed content that was at issue in the case. And an important part of that holding was that the automated features of the website that were written into the code, as opposed to any direct human involvement, were themselves enough to constitute content development under subsection (f)(3) of Section 230.

In the Second Circuit case that I noted in my testimony—that was FTC against LeadClick Media—the court followed the Ninth Circuit precedent, Roommates, and denied Section 230 immunity for the Internet marketer by deeming it a content developer, even though it didn't create the illegal content at issue; it merely provided advice to those who did create the content. That was deemed enough.

So, the fact that the same Second Circuit Court of Appeals reached the opposite result in the Force case shows how difficult that decision was, and how difficult it must have been, you know, on the facts. The plaintiffs argued that Facebook's algorithms had introduced terrorists to one another, and then they would have had the further burden of proving that Facebook was a knowing conspirator with the terrorists. That's what the Federal statute—it's a similar statute, 18 U.S.C. 2333—requires, or that Facebook, you know, knowingly participated in that situation. The Court seemed not to be persuaded that those facts had been adequately pleaded. But, they hung their hat on Section 230, as you point out. The facts alleged in the complaint seemed to make it appear that this was all the work of algorithms and the people at Facebook didn't themselves know that this happened, though they certainly found out about it eventually.

These are the kinds of cases involving the work of algorithms that I think are going to become more frequent. And so, in the future, it won't be enough, I think, to say that people didn't know that the algorithm did it. We were talking about this earlier. I think as AI takes over more and more responsibility for what we see on the Internet, the law is going to have to go one way or the other. Unless the people who write the algorithms are going to be responsible for what the algorithms do, everybody's quickly going to realize that that will be the easiest way to avoid any liability at all.

Whether it is possible to write a statute that cleanly parses when human knowledge is necessary, on the one hand, and when the work of an algorithm will be deemed to be the work of a human who could be held liable, on the other hand, that's a tough question. I think, in the medium- to short-run, this is going to be left for the courts to continue to sort out. And my hunch is that, as they've done in the Second Circuit, in the main, and the Ninth Circuit and elsewhere, that they're going to continue to look hard to find ways to ensure that wrongs don't go without remedies.

Mr. SYLVAIN. Can I answer your question, Senator Thune, about the Force case?

Senator THUNE. Yes.

Mr. SYLVAIN. So, if I had more space in the 5 minutes, I was going to talk about the Force case, for a couple of reasons I had already mentioned. It's a really interesting case out of the Second Circuit, for reasons Representative Cox mentions. But, I think it's no less interesting because of Chief Judge Katzmann's concurring opinion, in which he recognizes that the reasoning on which the majority of the panel bases its evaluation of whether or not Facebook should be subject to some liability in connection with the material support of terrorism because of recommendation algorithms, he doesn't agree with the conclusion, and he says that it's an invitation to Congress, an explicit invitation to Congress, to redress the emergent realities of automated decisionmaking systems for online intermediaries. Because, for him, he's not sure, as a matter of the way they're pled, as I think Representative Cox just said, that plaintiffs would have won, but this is a question that should have been resolved by the District Court after discovery had been gathered, to find out how deeply involved the recommendation algorithm was in the process. And I completely agree with Chief Judge Katzmann's approach to this.

I urge the members to look at the concurrence and think about ways of thinking about, you know, amending the statute. My impression is that the PACT Act does start this process, because, particularly in the context of complicated automated decisionmaking systems, regulators can be in a good position to evaluate consonance with public law.

Senator THUNE. Thank you, Mr. Sylvain.

Well, we would welcome your ongoing thoughts and suggestions and input with respect to some of these, as you described, novel situations, where, you know, we obviously want to get to see justice served. And I think the challenge that we face in all this, as I mentioned earlier, is protecting consumers and making sure that platforms, companies, have the ability to continue to innovate, and give

them room to maneuver, too, but in a way that ensures that consumers are protected.

So, that's a balance that we're trying to strike. I think the bill—as I said before, we've put a lot of thought and deliberation into trying to come up with a discrete set of solutions that we think get at some of these issues, but there are certainly exceptions, which will probably have to be, at some point, addressed, too, simply because of the continuing evolution of, as you all have pointed out, AI and algorithms and all these other ways now in which materials are being curated and made available to consumers.

So, we'll continue this discussion. I appreciate all of you contributing to it. Thank you.

And we will ask that members will have some time, a couple of weeks, to submit written questions for the record, and we would ask all of you, upon receipt of those questions, if you could submit your answers to the Committee as soon as possible. It would be greatly appreciated.

I would also like to submit a letter for the record from CCIA, EPIC, and OTIA. And those will be included in the hearing record, without objection.

[The information referred to follows:]

July 27, 2020

The Honorable John Thune
Chairman
Senate Committee on Commerce, Science, & Transportation
Subcommittee on Communications, Technology, Innovation and the Internet
Washington, DC 20510

The Honorable Brian Schatz
Ranking Member
Senate Committee on Commerce, Science, & Transportation
Subcommittee on Communications, Technology, Innovation and the Internet
Washington, DC 20510

Re: July 28 Subcommittee Hearing: The PACT Act and Section 230: The Impact of the Law that Helped Create the Internet and an Examination of Proposed Reforms for Today's Online World

Dear Chairman Thune and Ranking Member Schatz:

The undersigned organizations appreciate that the Subcommittee is carefully contemplating Section 230, and noting that it "helped create the Internet." Our organizations represent a wide range of companies that depend upon intermediary protections such as Section 230 to grow in the United States and export to markets around the world. Codified at 47 U.S.C. § 230, Section 230 facilitates legal online commerce and communication, encouraging millions of entrepreneurs and businesses to flourish. Section 230 also enables the companies we represent to invest substantial time and resources in developing and maintaining content moderation policies that protect consumers and promote free expression.

The U.S. legal framework for online services is critical to American leadership in the digital economy, promoting growth and innovation across sectors. The certainty provided by this framework reduces the threat of costly, likely ruinous litigation, enabling small U.S. businesses and startups to scale up quickly.[1] Undermining foundational intermediary liability protections would cost 4.25 million American jobs and $400 billion over the next decade, according to 2017 research.[2]

Intermediary liability protections also play a key role in enabling American small businesses to build trust and customer relationships in new markets. Today, millions of U.S. small businesses are taking advantage of online commerce to reach far beyond local markets, including through marketing tools and interactive customer services. However, for these tools to function,

[1] Engine, *Section 230: Cost Report* (2019), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5c8168cae5e5f04b9a30e84e/1551984843007/Engine_Primer_230cost2019.pdf.

[2] Christian Dippon, *Economic Value of Internet Intermediaries and the Role of Liability Protections* (NERA 2017), http://internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protections.pdf.

companies need legal certainty that they will not be held liable for all communications that arise between businesses and consumers using these tools.

Section 230 enables online services, websites, and many other digital intermediaries to maintain healthy and vibrant ecosystems. It is both a sword and shield against bad actors, limiting liability pertaining to third-party content or behavior, while also enabling services to act promptly against unlawful or injurious content or misbehavior. By protecting intermediary decisions whether content is removed or not, Section 230 encourages services to fight misconduct and protect users from online harms by removing disincentives to moderate. This helps combat online content and misbehavior that is abusive, inappropriate, or otherwise objectionable, though lawful. Narrowing this protection would have the perverse result of impeding online services' and websites' efforts to police bad actors and misconduct, including key consumer protections that users have come to expect, such as spam filtering.

Weakening Section 230 protections would be likely to produce different responses from different online services. Smaller operators may avoid moderating content at all because online services have less legal liability if they engage in no monitoring. As demonstrated in the 1995 *Stratton Oakmont* decision that Section 230 overturned, removing 99% of inappropriate content could create the appearance of endorsing the 1% that an online service overlooked. An additional outcome may be that firms would exit the market — or never enter it — which would discourage innovation and free expression by all stakeholders and viewpoints. Another likely result would be even more aggressive editorial policies. Cautious sites and services, wary of anything that could lead to risk, may only give a platform to establishment viewpoints.

Section 230 also empowers law enforcement to take actions against service providers for anything that is unlawful including any violations of federal criminal law, intellectual property law, illegal trafficking of drugs or weapons, and child protection law.[3] It should go without saying that if something is illegal offline, it is also illegal online. The speaker is *always* liable for the illegal activity and the service is also liable if there is a violation of federal criminal law, IP law, or any of the other exemptions to Section 230. At the same time, if a service "is responsible in whole or in part for the creation or development" of the content, Section 230 is no protection.[4]

Thank you very much for your thoughtful consideration of these important issues. We look forward to continuing to work with you as Congress considers Section 230.

Sincerely,

Computer & Communications Industry Association
Consumer Technology Association
Engine
Internet Infrastructure Coalition

Cc: Members of the Subcommittee on Communications, Technology, Innovation and the Internet

[3] *See* 47 U.S.C. § 230(e)(1)-(5).
[4] *Id.* § 230(f)(3). This is what allowed the FBI to take down Backpage even before enactment of FOSTA.

Senator THUNE. So, thank you all very much. I think this was very constructive and helpful, and it certainly will inform our decisions as we figure out how to proceed here. And I hope that we can proceed. I do believe it's time, and I think there are a lot of good ideas out there that we can include in a potential solution.

So, thank you all very much.

This hearing is adjourned.

[Whereupon, at 12:42 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. SHELLEY MOORE CAPITO TO JEFF KOSSEFF

Are you aware of any instance where an interactive computer service has profited from illegal activity online? If so, which services? What have they done to remedy these instances?

Answer. My response is only my personal view, as a Section 230 scholar, and does not represent the views of the Naval Academy, Department of Navy, Department of Defense, or any other party.

Online crime is a serious problem. Just as in the offline world, illegal activity can and does occur in cyberspace. For instance, the U.S. Senate Permanent Subcommittee on Investigations concluded in a January 2017 report that online classified advertising site Backpage.com "knows that advertisers use its site extensively for child sex trafficking, but the company has often refused to act swiftly in response to complaints about particular underage users—preferring in some cases to interpret these complaints as the tactics of a competing escort."[1] The U.S. Court of Appeals for the First Circuit ruled in 2016 that Section 230 barred civil claims against Backpage.com by victims who were trafficked on the site, causing Congress in 2018 to amend Section 230 to allow certain civil claims and state criminal enforcement.[2] It is important to note, however, that Section 230 always has had an exception for the enforcement of Federal criminal law,[3] allowing the Justice Department to seize Backpage.com a few days before the Section 230 amendment was signed into law.

Many other online crimes also pose a constant challenge for law enforcement. Among the most serious is the distribution of child sex abuse material. Online platforms must file reports if they obtain actual knowledge of apparent violations of child sex abuse material laws.[4] The service providers are not legally required to monitor for child sex abuse material,[5] and such a requirement could raise Fourth Amendment concerns.[6] Nonetheless, many platforms voluntarily use technology such as PhotoDNA to scan for illegal content. The challenge for all of us who are concerned about online crime is to encourage the development and deployment of such technologies without disturbing the very delicate Fourth Amendment balance that allows these systems to detect online crime.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RICK SCOTT TO JEFF KOSSEFF

Mr. Kosseff, do you think social media platforms, like Twitter or Facebook, should be able to restrict free speech and expression online to a greater extent than our First Amendment? And if so, why should they benefit from Section 230s legal immunity provision that was intended to promote free speech online?

Answer. My response is only my personal view, as a Section 230 scholar, and does not represent the views of the Naval Academy, Department of Navy, Department of Defense, or any other party.

Yes. Some content, such as hate speech, is constitutionally protected yet quite harmful. Online platforms should be able to protect their users from such harm. Prohibiting a platform from engaging in certain forms of moderation could raise independent First Amendment concerns, as would tying a government benefit such as liability protection to a certain form of moderation.

---

[1] UNITED STATES SENATE, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS, BACKPAGE.COM'S KNOWING FACILITATION OF ONLINE SEX TRAFFICKING (Jan. 9, 2017) at 3.

[2] Doe No. 1 v. Backpage. com, LLC, 817 F. 3d 12 (1st Cir. 2016).

[3] 47 U.S.C. § 230(e)(1).

[4] 18 U.S.C. § 2258A.

[5] 18 U.S.C. § 2258A(f).

[6] *See* United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016).

One of Section 230s findings was that the "Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activities,"[7] a recognition of the role that Section 230 could play in enabling online speech. Yet Congress also explicitly stated that Section 230 was intended to overturn a New York state trial court decision that suggested that a platform faces increased liability for all user content by engaging in some content moderation.[8] In other words, Congress wanted platforms to determine how to moderate content in the manner that their users demanded. To that end, Section 230 assumes that if platforms fail to meet users' expectations (either by over-moderating or under-moderating), users will seek other platforms.

It is fair to question whether the Internet created by Section 230 works fairly when a handful of platforms have billions of users and control a great deal of online speech. Are other platforms available if users are unhappy with a company's moderation practices? Being suspended or banned from one of these platforms can have a dramatic impact on a person's ability to speak and, in some cases, earn a living. A suspension from Prodigy or CompuServe in 1996 simply would not have the same impact.

I cannot say with any degree of certainty what impact a repeal of or significant amendment to Section 230 would have on moderation. It is unclear how courts would apply the common law and First Amendment protections for distributors of third-party content to modern platforms, as Section 230 has been on the books since 1996. Until we know the rules in a Section 230-free world, we do not know how platforms would respond. There is a chance that at least some platforms would reduce the avenues for user generated content, fearing increased liability, or they might increase their moderation and block more content that is on the margins. Conversely, platforms might engage in less moderation, fearing that any involvement might make them liable for all user content. It also is conceivable that only the largest platforms could survive in a world without Section 230, eliminating smaller competitors and further consolidating venues for online speech.

○

[7] 47 U.S.C. § 230(a)(3).

[8] Stratton Oakmont v. Prodigy Service Co., 23 Media L. Rep. 1794 (N.Y. Sup. Ct. May 24, 1995).